RINGS WITH GENERALIZED IDENTITIES

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. Więslaw,* 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. Darnel,* 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

Additional Volumes in Preparation

RINGS WITH GENERALIZED IDENTITIES

K. I. Beidar
National Cheng-Kung University
Tainan, Taiwan

W. S. Martindale III
University of Massachusetts
Amherst, Massachusetts

A. V. Mikhalev
Moscow M. V. Lomonosov State University
Moscow, Russia

Marcel Dekker, Inc. New York • Basel • Hong Kong

Library of Congress Cataloging-in-Publication Data

Beidar, K. I. (Konstantin I.).
Rings with generalized identities / K. I. Beidar, W. S. Martindale III, A. V. Mikhalev.
p. cm. — (Monographs and textbooks in pure and applied mathematics ; 196)
Includes index.
ISBN 0-8247-9325-0 (alk. paper)
1. Polynomial rings. I. Martindale, W. S. (Wallace S.). II. Mikhalev, A. V. (Aleksandr Vasil′evich). III. Title. IV. Series.
QA251.3.B45 1995
512'.4—dc20 95-40715
CIP

This book is printed on acid-free paper.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

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

PRINTED IN THE UNITED STATES OF AMERICA

Preface

A generalized polynomial identity (GPI) of an algebra A over a field F is a polynomial expression f in noncommutative variables and fixed coefficients from A between the variables such that f vanishes upon all substitutions by elements of A. It is a natural extension of the notion of a polynomial identity (PI), in which the coefficients come from the base field F. The theory of GPI's is in reality, however, quite separate from that of ordinary PI's. It is a rather rare occurrence that results in GPI theory provide better proofs or insight into PI results. Rather, the usefulness of GPI theory lies in the fact that in many problems in noncommutative ring theory involving elementwise calculations GPI's appear frequently and naturally, whereas PI's seldom make their appearance. Of course one expects PI's to have a stronger effect on a ring than do GPI's, and this shows up very clearly in the case of a primitive ring R, i.e., a dense ring of linear transformations of a vector space V over a division ring D. Here the presence of a PI forces R to be finite dimensional central simple whereas a GPI, though forcing R to have minimal right ideals and D to be finite dimensional over its center, has no effect on the dimension of V over D. As a special case one has the ring R of all linear transformations of an infinite dimensional vector space over a field. If e is a rank one idempotent then R satisfies the GPI $exeye = eyexe$ for all x and y in R whereas R satisfies no PI.

Just as *PI* theory began with Kaplansky's 1948 paper on primitive *PI* rings, the theory of *GPI*'s was initiated by Amitsur in 1965 with his fundamental paper on primitive *GPI* rings. In 1969 Martindale extended Amitsur's work to prime *GPI* rings. A key notion in making the transition to a prime ring R was that of the extended centroid C and the resulting central closure RC, it becoming clear that C (rather than the field of fractions of the centroid) was the proper field of scalars in the case of prime rings. A short time later generalizations in two directions occurred. In one *GPI*'s involving involutions were studied by Martindale, Rowen, and others, and in another *GPI* theory was extended to semiprime rings by Beidar and Mikhalev using the technique of orthogonal completion, a powerful alternative to the usual method of reducing semiprime problems to prime rings.

One of the most significant advances was made in a series of fundamental papers by Kharchenko in the late 1970's in which *GPI*'s involving derivations and automorphisms were studied, i.e., the variables were suggestively superscripted by compositions of derivations and automorphisms. (Let us henceforth refer to these more complicated identities simply as generalized identities (*GI*'s)). Indeed, Utumi's (1956) ring of quotients of a ring R was seen to contain elements which induce automorphisms and derivations in R (called X-inner automorphisms and derivations in honor of Kharchenko). In 1985 Lanski investigated the situation of *GI*'s in prime rings with involution. Around 1990 Chuang carried the theory to its present state by adding arbitrary antiautomorphisms to the Kharchenko results. He introduced the important notion of Frobenius (anti)automorphism for prime rings using which he gave a description of the structure of (not necessarily multilinear) *GI*'s involving derivations and (anti)automorphisms, thus extending Kharchenko's results even in the case of derivations and automorphisms.

The centerpiece of this book is Chapter 7 in which the theorems of Kharchenko and Chuang on *GI*'s in prime rings are presented. Special attention is paid to describing the "home" of GI's (a matter which is somewhat glossed over in the accounts of Kharchenko and Chuang). Also presented in this chapter is a striking application of Kharchenko's results to the characterization of algebraic derivations and automorphisms. The extension of the results of Chapter 7 to semiprime rings is accomplished in Chapter 8.

The choice of topics for Chapters 1 through 5 is generally dictated by what is needed for the exposition in Chapters 6 through 9. As mentioned earlier the extended centroid plays a key role in the definition of a GI and a detailed discussion of its properties is included in Chapter 2. It has also been pointed out that certain rings of quotients (notably the symmetric ring of quotients, a subring of Utumi's ring of quotients) are also needed in order to properly define GI's, and accordingly a general account of rings of quotients is also given in Chapter 2. The "home" for GI's is a certain coproduct, and this notion is discussed in some detail in Chapter 1. A generalized Poincaré-Birkhoff-Witt theorem (PBW theorem) for differential Lie algebras is precisely what is needed for characterizing nontrivial GI's involving derivations, and this topic forms the content of Chapter 5. The main tool used in our proof of the PBW theorem is the Diamond Lemma and we therefore present a careful exposition of this result in Chapter 1. The interplay between derivations and (anti)automorphisms leads naturally to skew group rings, which are briefly summarized in Chapter 1. The extension of GI results to semiprime rings requires the theory of orthogonal completion (developed by Beidar and Mikhalev), and this subject, along with a review of first order logic in Chapter 1, is laid out in Chapter 3. Since the effect of a nontrivial GI on a prime ring is to force its central closure to have minimal right ideals, we have given a fairly detailed account of primitive rings with nonzero socle in Chapter 4.

GPI's are of course just a special case of GI's in which derivations and (anti)automorphisms are not involved, and various results on GPI's are presented in Chapter 6. Included here is a very short proof (due to Chuang) of Martindale's result on prime GPI rings. To help prepare the reader for the transition from GPI's to the far more involved GI's of Chapter 7, we also present in Chapter 6 various results on GPI's with involution. The generators of the T-ideal of GPI's in prime rings have been determined by Beidar and an account of this is given here. At the end of Chapter 6 several results on special GPI's are presented.

A powerful feature of GPI theory is that frequently one can (so to speak) have the best of both worlds: if the particular GPI is nontrivial then the ring is tractable (e.g., has nonzero socle) whereas if the GPI is trivial there is often a strong relation among the coefficients. A striking example of this phenomenon occurs in the recent solution of a long-standing conjecture of Herstein on Lie isomorphisms, which we present in Chapter 9. We also give here some details of the theory of n-additive commuting maps initiated by Bresar, which is a powerful tool in combinatorial ring theory and plays an important role in the Lie isomorphism problem.

Some comments for the reader's benefit are now in order. The subject matter of this book in its full generality, i.e., GI's with derivations and (anti)automorphisms in a semiprime setting, is admittedly both mathematically and notationally complicated. However, depending on the particular reader's interests and concerns, some of this burden may be alleviated. Most notably, for the reader solely interested in prime rings, a considerable portion of the material may be bypassed, namely, Section 1.6, Chapters 3 and 8, and those parts of Chapter 6 concerned with semiprime rings. Furthermore, without too much effort, most of the statements of the main results of Chapters 5, 6 and 7 can be easily understood and in fact have a natural intuitive appeal (even though lengthy rigorous proofs may be required).

The various Poincaré-Birkhoff-Witt theorems in Chapter 5 are a case in point. Another example is the set of "obvious" generators of the T-ideal of GPI's in Chapter 6. The main results of the book, to be found in Sections 7.5, 7.6 and 7.7, have rather short simple statements, and the very definition of a generalized identity and its "reduction" to a prescribed "nontrivial" form are often dismissed as being too self-evident to warrant much attention. At any rate the reader should not have the idea that Chapters 1 through 6 must be read line by line before he or she is able to find out (in Chapter 7) what the title of the book means!

With the book having already reached critical length, we have decided not to include a chapter on generalized rational identities. Another topic we shall not discuss is that of Galois theory of prime and semiprime rings. This subject is thoroughly treated in the recent book of Kharchenko, "Automorphisms and derivations of associative rings" (Kluwer, 1991). Various results on GPI's (with involution) are also to be found in Rowen's book, "Polynomial identities in ring theory" (Academic Press, 1980). GPI's are touched upon very briefly in Procesi's book, "Rings with polynomial identities" (Marcel Dekker, 1973).

The authors wish to extend their appreciation to the University of Massachusetts (Amherst), Moscow State University (Moscow), National Taiwan University (Taipei), and National Cheng-Kung University (Tainan) for use of their facilities and for hosting the authors. The content of some chapters was discussed at research seminars at the University of Massachusetts, at the Moscow State University, at the University of Southern California, at the National Cheng-Kung University and at the National Taiwan University, and we express our thanks to leaders and participants of these algebraic seminars, and especially to P. H. Lee, Y. Fong, C. L. Chuang, W.-F. Ke, S. Montgomery, V. N. Latyshev, Ch. Lanski and V. T. Markov. We are thankful to A. A. Mikhalev for his assistance in discussion of some arguments of Chapter 5 and to M. A. Chebotar for his help in writing a part of Section 7.9. We benefitted also from the efforts of P. Blau, who carefully read the manuscript and pointed out numerous corrections incorporated in the text. We are grateful to W.-F. Ke for invaluable help in preparing the TEX version of this book. Finally, we are grateful to our publisher, Marcel Dekker, Inc., for being lenient about deadlines and understanding the communication problems between authors located many thousands of miles apart.

K. I. Beidar
W. S. Martindale III
A. V. Mikhalev

Contents

This Page Intentionally Left Blank

RINGS WITH GENERALIZED IDENTITIES

This Page Intentionally Left Blank

Chapter 1

Preliminaries

1.1 Basic Notions

In this book we shall mainly be concerned with three types of rings. A ring R is *prime* if, for any two ideals U and V of R, $UV = 0$ implies $U = 0$ or $V = 0$. As a special case of a prime ring, a ring is *(right) primitive* if it has a faithful irreducible right R-module. As a generalization of a prime ring, a ring R is *semiprime* if it has no nonzero nilpotent ideals. We will assume the reader is familiar with these concepts and with equivalent formulations thereof. We point out that prime (resp. primitive) rings are the basic "building blocks" in the structure theory of rings if one takes as the *radical* the *Baer lower* (resp. *Jacobson*) radical. A semiprime ring can always be written as a subdirect product of prime rings. However, a much more powerful method of reducing questions about rings to prime rings is the method of *orthogonal completion* (which will be developed in Chapter 3 and applied in Chapter 9).

Let K be a commutative ring with 1. By definition a *K-ring* A is a ring with 1 for which there exists a ring homomorphism $\sigma : K \to A$ (sending 1 to 1). It follows that A is a unital (K, K)-bimodule by defining $ka = k^\sigma a$ and $ak = ak^\sigma$, $a \in A$, $k \in K$.

As an important example, if R is a ring with center C, then $A = End(R)$ (the ring of endomorphisms of the additive group R) is a C-ring by letting c^σ be the left multiplication of R by c, $c \in C$.

We will define a *K-algebra* A to be a K-ring in which K^σ is contained in the center of A (this is equivalent to the usual definition of an algebra with 1 over K). In case σ is injective (which will usually be the case) we shall assume that A contains K. Of particular interest to us is the situation where K is a field (when we study prime rings) or the more general situation where K is a *von Neumann regular self-injective* ring (when we study semiprime rings). Here we recall that K is *self-injective* if it is injective as a K-module. In case A contains K and K is self-injective it can be shown that $K \cdot 1$ is a K-direct summand of the algebra A.

A *derivation* of a ring R is an additive map $\delta : R \to R$ such that $(xy)^\delta = x^\delta y + xy^\delta$ for all $x, y \in R$. For $a \in R$ the mapping μ given by $x^\mu = [a, x] = ax - xa$ is easily seen to be a derivation and is called *inner* (sometimes denoted by $ad(a)$ or $[a, \ ]$). It is straightforward to show that the set $Der(R) \subseteq End(R)$ of all derivations is a *Lie ring*, i.e., is closed under addition and the Lie product $[\delta, \tau]$.

Given a natural number n, we set $\mathcal{E}_n$ equal to the set of all subsets of $W(n) = \{1, 2, \ldots, n\}$. For derivations $\delta_1, \delta_2, \ldots, \delta_n \in Der(R)$ and a subset $S = \{j_1, j_2, \ldots, j_k\} \in \mathcal{E}_n$, where $j_t < j_{t+1}$ for all $t < k$, we let Δ_S denote the product $\delta_{j_1}\delta_{j_2}\ldots\delta_{j_k}$ and Δ'_S denote $\Delta_{W(n)\setminus S}$. It will be useful to have at our disposal the following

Remark 1.1.1 (Leibnitz Formulas) *(a) For all $x, y \in R$, $\delta_1, \delta_2, \ldots, \delta_n \in Der(R)$, and $\Delta = \delta_1\delta_2\ldots\delta_n$ the following equality holds*

$$(xy)^\Delta = \sum_{S \in \mathcal{E}_n} x^{\Delta_S} y^{\Delta'_S}.$$

***(b)** (special case of **(a)**) For $x, y \in R$ and $\delta \in Der(R)$*

$$(xy)^{\delta^n} = \sum_{i=0}^{n} \binom{n}{i} x^{\delta^i} y^{\delta^{n-i}}.$$

(It is understood that $\Delta_\emptyset$ and δ^0 mean 1).

The proof is by induction on n and we leave the straightforward though notationally complicated details to the reader.

As an immediate corollary to Remark 1.1.1(b) we see that in characteristic p (p a prime) $Der(R)$ is also closed under pth powers $\delta \mapsto \delta^p$.

Other mappings of major interest to us are the *automorphisms* and *antiautomorphisms* of R. An important special case is an *involution* of R, i.e., an antiautomorphism of period 1 or 2. We will denote the set of all automorphisms (resp. antiautomorphisms) of R by $Aut(R)$ (resp. $Antiaut(R)$). It is easily seen that $G(R) = Aut(R) \cup Antiaut(R)$ is a group.

The center $Z(R)$ of R is also an important set, and we may (and often will) regard $Z(R)$ as acting on R via left multiplications.

If σ is a homomorphism of rings $K \to T$ and ${}_KV, {}_TW$ are modules then an additive map $\phi : V \to W$ is called *σ-semilinear* if $(kv)^\phi = k^\sigma v^\phi$, $k \in K$, $v \in V$. Analogously if μ is a derivation of K, an additive map $\phi : V \to V$ is called *μ-semilinear* if $(kv)^\phi = k^\mu v + kv^\phi$, $k \in K$, $v \in V$.

A *derivation* δ of a K-algebra A will mean a derivation of the ring A; we do not assume that δ is necessarily K-linear. In case μ is a derivation of K then a derivation δ of A is called a *μ-derivation* of A if δ is also a μ-semilinear map, i.e., $(ka)^\delta = k^\mu a + ka^\delta$, $k \in K$, $a \in A$. In a similar fashion an *automorphism* (*antiautomorphism*) g of a K-algebra will mean an automorphism (antiautomorphism) of the ring A. If

σ is an automorphism of K then g is a *σ-automorphism* (*σ-antiautomorphism*) of A if g is also a σ-semilinear map, i.e., $(ka)^g = k^\sigma a^g$.

We continue this section with a brief discussion of *skew group rings*. For us the motivating example for this notion comes from two simple "skew" relationships connecting $Der(R)$, $G(R)$ and $Z(R)$ (all contained in $End(R)$). Let $x, y \in R$, $\delta \in Der(R)$, $g \in G(R)$ (we will just consider the case where g is an antiautomorphism). We then see from the equations

$$\begin{aligned}(xy)^{g^{-1}\delta g} &= \left(y^{g^{-1}} x^{g^{-1}}\right)^{\delta g} = \left(y^{g^{-1}\delta} x^{g^{-1}} + y^{g^{-1}} x^{g^{-1}\delta}\right)^{g} \\ &= x y^{g^{-1}\delta g} + x^{g^{-1}\delta g} y\end{aligned}$$

that

Remark 1.1.2 *$g^{-1}\delta g$ is an element of $Der(R)$ (notation: $\delta^g = g^{-1}\delta g$).*

Similarly, for $c \in Z(R)$, we see from $c^g x^g = x^g c^g$ and $x^{g^{-1}cg} = \left(c x^{g^{-1}}\right)^g = c^g x$ that

Remark 1.1.3 *$c^g \in Z(R)$ and $c^g = g^{-1}cg$.*

We proceed now to recall the notion of *skew group ring*. Let R be a ring with 1, G a group, and $\psi : G \to Aut(R)$ a group homomorphism. We refer to ψ as an *action* of G on R. However, we will usually suppress the ψ and simply write r^g for $r^{(g^\psi)}$. The *skew group ring* $R \propto G$ of R and G is then defined to be the free left R-module with basis G, where multiplication is given according to $gr = r^{g^{-1}} g$ and its consequences. It is straightforward to verify that $R \propto G$ is in fact a ring. Now let A be a ring with 1, α a ring homomorphism of R into A, and β a group homomorphism of G into the multiplicative semigroup of A sending 1 to 1. Clearly the map $\gamma : R \propto G \to A$ given by $\sum r_g g \mapsto \sum r_g^\alpha g^\beta$ is a well-defined additive map. A useful criteria for γ to be a ring homomorphism is given by

Lemma 1.1.4 *A necessary and sufficient condition for γ to be a ring homomorphism is the following: if R is generated as a ring by a subset X then*

$$x^\alpha g^\beta = g^\beta x^{g\alpha}, \quad x \in X,\ g \in G.$$

Proof. If γ is a homomorphism then from

$$x^\alpha g^\beta = (xg)^\gamma = (gx^g)^\gamma = g^\gamma \left(x^g\right)^\gamma = g^\beta x^{g\alpha}$$

the necessity is clear. To show the sufficiency, since X generates R as a ring, we need only show that $(uv)^\gamma = u^\gamma v^\gamma$ for $u = x_1 x_2 \ldots x_n g$ and $y = y_1 y_2 \ldots y_m h$, $x_i, y_j \in X$, $g, h \in G$. We then have

$$\begin{aligned}
(uv)^\gamma &= \left(x_1 \ldots x_n y_1^{g^{-1}} \ldots y_m^{g^{-1}} gh\right)^\gamma \\
&= \left(x_1 \ldots x_n y_1^{g^{-1}} \ldots y_m^{g^{-1}}\right)^\alpha (gh)^\beta \\
&= x_1^\alpha \ldots x_n^\alpha y_1^{g^{-1}\alpha} \ldots y_m^{g^{-1}\alpha} g^\beta h^\beta = x_1^\alpha \ldots x_n^\alpha g^\beta y_1^\alpha \ldots y_m^\alpha h^\beta \\
&= (x_1 \ldots x_n)^\alpha g^\beta (y_1 \ldots y_m)^\alpha h^\beta = u^\gamma v^\gamma
\end{aligned}$$

and the proof is complete.

We close this section with a "weak density" theorem which will have important applications in several places later on. The motivation comes from the celebrated Jacobson Density Theorem; the reader will notice that virtually the same proof can be used.

For a ring S let N be a right S-module, let $\Delta = End(N_S)$ (thus N is a (Δ, S)-bimodule), let ${}_\Delta M$ be a left Δ-module, and let T be an S-submodule of the right S-module $Hom({}_\Delta M, {}_\Delta N)$.

We shall refer to the above system as a *(right) S-context*. With reference to this S-context we make three definitions:

N is *closed:* given any homomorphism of S-modules $f : U_S \to N_S$ (where $0 \neq U_S$ is a submodule of N_S) there exists $\lambda \in \Delta$ such that $\lambda u = f(u)$ for all $u \in U$. (Note that *closed* simply means *quasi-injective*).

T is *total:* for any $0 \neq m \in M$ we have $mT \neq 0$.

T is *weakly dense:* given $m_1, m_2, \ldots, m_k \in M$, with $m_1 \notin \sum_{i=2}^{k} \Delta m_i$, there exists $t \in T$ such that $m_1 t \neq 0$, $m_i t = 0$ for $i > 1$.

In an analogous fashion one may define a *left S-context* with a similar ensuing discussion.

Theorem 1.1.5 (Weak Density Theorem) *Given an S-context as above such that N_S is closed and T is total, then T is weakly dense.*

Proof. We proceed by induction on k. The case $k = 1$ is clear because T is total. Now let $m_1 \notin \sum_{i=2}^{k} \Delta m_i$. Suppose the result is not true, i.e., for all $t \in T$ $m_1 t = 0$ whenever $m_i t = 0$ for all $i = 2, 3, \ldots, k$. We set $J = \{t \in T \mid m_i t = 0,\ i > 2\}$ (if $k = 2$ set $J = T$). Clearly J is an S-submodule. If $m_2 \in \sum_{i=3}^{k} \Delta m_i$ then we are finished immediately by the induction hypothesis. Therefore, again by the induction hypothesis, $m_2 J \neq 0$, and $m_2 J$ is an S-submodule of N_S. We define $f : m_2 J \to N$ by the rule $m_2 t \mapsto m_1 t$ for all $t \in J$. f is well-defined, since if $m_2 t = 0$ we have $m_1 t = 0$ by our earlier assumption. Certainly f is an S-module map and so (since N_S is closed) there exists $\lambda \in \Delta$ such that $\lambda(m_2 t) = f(m_2 t) = m_1 t$ for all $t \in J$, i.e., $(\lambda m_2 - m_1)J = 0$. But then consider the elements $\lambda m_2 - m_1, m_3, \ldots, m_k$. Since $m_1 \notin \sum_{i=2}^{k} \Delta m_i$, $\lambda m_2 - m_1 \notin \sum_{i=3}^{k} \Delta m_i$. By the induction hypothesis we would have $(\lambda m_2 - m_1)J \neq 0$, and so we have reached a contradiction.

1.2 Tensor Products and Free Algebras

Let K be a commutative ring with 1, let V be a right K-module and let W be a left K-module. For P any additive abelian group we say that a map $\phi : V \times W \to P$ is *balanced* if it is biadditive and satisfies $(v\alpha, w)^\phi = (v, \alpha w)^\phi$, $\quad v \in V, \quad w \in W, \quad \alpha \in K$. An abelian group T is called a *tensor product* of V and W over K if the following properties hold:

(i) *There is a balanced map $\tau : V \times W \to T$ such that T is additively generated by the image of τ.*

(ii) *Given any abelian group P and any balanced map $\rho : V \times W \to P$ there exists an additive map $\psi : T \to P$ such that $\rho = \tau\psi$.*

The existence of such a T is easily seen as follows. Let F be the free abelian group on the *set* $V \times W$, and let N be the subgroup of F generated by all elements of the form

$$\begin{aligned}
&(v_1 + v_2, w) - (v_1, w) - (v_2, w)\\
&(v, w_1 + w_2) - (v, w_1) - (v, w_2)\\
&(v\alpha, w) - (v, \alpha w), \quad v, v_1, v_2 \in V,\ w, w_1, w_2 \in W,\ \alpha \in K.
\end{aligned}$$

We claim that $\overline{F} = F/N$ is a tensor product of V and W over K. Indeed, the map $\tau : (v, w) \mapsto \overline{(v, w)} = (v, w) + N$ fulfills condition (i). For a mapping $\rho : (V, W) \to P$ balanced, define $\chi : F \to P$ according to $(v, w) \mapsto (v, w)^\rho$. Since χ maps N to 0 it induces the desired additive map $\psi : \overline{F} \to P$ satisfying (ii). The uniqueness of the tensor product (up to isomorphism) is easily seen from consideration of the commutative diagram

$$\begin{tikzcd}
V \times W \arrow[r, "\tau"] \arrow[dr, "\tau'"'] & T \arrow[d, shift right, "\psi"'] \\
& T' \arrow[u, shift right, "\psi'"']
\end{tikzcd}$$

showing that ψ and ψ' are inverses of each other. We will denote the tensor product of V and W over K by $V \otimes_K W$ and a typical generator $(v, w)^\tau$ by $v \otimes w$.

Suppose furthermore that W is a (K, L)-bimodule for some commutative ring L. Then $V \otimes_K W$ is a right L-module with multiplication given by $(v \otimes w)l = v \otimes wl, \quad l \in L$. The well-definedness of this operation follows from the fact that for $l \in L$ the map $\rho : (v, w) \mapsto v \otimes wl$ is balanced. In particular, if V and W are K-modules, $V \otimes_K W$ is again a K-module.

Given one or more K-modules $V, W, \ldots$ we will find it useful to form the *tensor algebra* determined by these modules over K. We proceed to briefly describe this construction for the case of two modules V and W.

First consider a fixed ordered sequence $S_1, S_2, \ldots, S_n$ where for each $i = 1, 2, \ldots, n \quad S_i = V$ or $S_i = W$. We define the *n-fold tensor product* to be that K-module S characterized by the properties:

(i)′ *There is an n-linear map $\tau : S_1 \times \ldots \times S_n \to S$ whose image generates S additively.*

(ii)′ *Given $\phi : S_1 \times \ldots \times S_n \to P$ any n-linear map into a K-module P, there exists a K-linear map $\psi : S \to P$ such that $\phi = \tau\psi$.*

One shows the existence and uniqueness of S in a similar manner as earlier; we denote this n-fold tensor product by $S = S_1 \otimes \ldots \otimes S_n$.

We now define the *tensor algebra* T of V and W over K to be the direct sum of all the n-fold tensor products:

$$\begin{aligned} T &= K \oplus V \oplus W \oplus (V \otimes V) \oplus (V \otimes W) \oplus (W \otimes V) \\ &\quad \oplus (W \otimes W) \oplus (V \otimes V \otimes V) \oplus \dots. \end{aligned}$$

Clearly the problem of defining multiplication reduces to the following situation. Let $S_{(n)} = S_1 \otimes \dots \otimes S_n$, $S'_{(m)} = S'_1 \otimes \dots \otimes S'_m$, and $S_{(m+n)} = S_1 \otimes \dots \otimes S_n \otimes S'_1 \otimes \dots \otimes S'_m$, where each S_i, S'_j is either V or W. If $s = (s_1, \dots, s_n) \in S_1 \times \dots \times S_n$, $t = (t_1, \dots, t_m) \in S'_1 \times \dots \times S'_m$ we let $\bar{s} = s_1 \otimes \dots \otimes s_n \in S_{(n)}$, $\bar{t} = t_1 \otimes \dots \otimes t_m \in S'_m$. We define a binary operation $S_{(n)} \times S_{(m)} \to S_{(m+n)}$ as follows: for $x = \sum_s \bar{s}$, $y = \sum_t \bar{t}$ we set $xy = \sum_{s,t} \bar{s} \otimes \bar{t}$. We shall show this is well-defined, leaving associativity, etc., to the reader. Indeed, for each $t \in S'_1 \times \dots \times S'_m$ there is a K-linear map $\psi_t : S_{(n)} \to S_{(m+n)}$ given by $x^{\psi_t} = \sum_s \bar{s} \otimes \bar{t}$, and for each $s \in S_1 \times \dots \times S_n$ there is a K-linear map $\chi_s : S'_{(m)} \to S_{(m+n)}$ given by $y^{\chi_s} = \sum_t \bar{s} \otimes \bar{t}$. Now suppose $x = \sum_s \bar{s} = \sum_u \bar{u}$ and $y = \sum_t \bar{t} = \sum_v \bar{v}$. Then

$$\begin{aligned} \sum_{s,t} \bar{s} \otimes \bar{t} &= \sum_t \left(\sum_s \bar{s} \otimes \bar{t} \right) = \sum_t x^{\psi_t} = \sum_t \left(\sum_u \bar{u} \otimes \bar{t} \right) \\ &= \sum_{u,t} \bar{u} \otimes \bar{t} = \sum_u y^{\chi_u} = \sum_u \left(\sum_v \bar{u} \otimes \bar{v} \right) = \sum_{u,v} \bar{u} \otimes \bar{v}. \end{aligned}$$

In case we are dealing only with a single K-module V we shall denote the tensor algebra determined by V over K as $K\{V\}$.

In the following remarks V is a K-module, K a commutative ring with 1.

Remark 1.2.1 *Let P be a K-algebra and let $\phi : V \to P$ be a K-linear map. Then ϕ can be uniquely extended to a K-algebra map $\psi : K\{V\} \to P$.*

Proof. Using property $(ii)'$ the map $\chi : V \otimes \ldots \otimes V \to P$ given by $v_1 \otimes \ldots \otimes v_n \mapsto v_1^\phi v_2^\phi \ldots v_n^\phi$ is a well-defined K-linear map, and extension of χ by additivity to $K\{V\}$ yields the required K-algebra map ψ.

Corollary 1.2.2 *Let σ be an automorphism of K, let P be a K-algebra, and let $\phi : V \to P$ be a σ-semilinear map. Then:*

(a) ϕ can be uniquely extended to a σ-homomorphism of K-algebras $\psi : K\{V\} \to P$.

(b) ϕ can be uniquely extended to a σ-antihomomorphism of K-algebras $\psi : K\{V\} \to P$.

Proof. To prove (a) we consider P as a K-algebra P^* by defining $k \cdot x = k^\sigma x, \quad k \in K, \quad x \in P$. Then $\phi : V \to P^*$ is a K-linear map and so by Remark 1.2.1 may be extended to a K-algebra map $\psi : K\{V\} \to P^*$, i.e., a σ-homomorphism $\psi : K\{V\} \to P$. To prove (b) let P^o be the opposite algebra of P. Then by part (a) ϕ can be uniquely extended to a σ-homomorphism $\psi : K\{V\} \to P^o$, i.e., a σ-antihomomorphism $\psi : K\{V\} \to P$.

Corollary 1.2.3 *Let δ be a derivation of K and let $\phi : V \to K\{V\}$ be a δ-semilinear map. Then ϕ can be uniquely extended to a δ-derivation μ of $K\{V\}$.*

Proof. Set $T = K\{V\}$, let A be the set of all matrices of the form $a = \begin{pmatrix} s & t \\ 0 & s \end{pmatrix}, \quad s, t \in T$, and let K' be the set of all matrices of the form $k' = \begin{pmatrix} k & k^\delta \\ 0 & k \end{pmatrix}, \quad k \in K$. One readily checks that $K \cong K'$ via the map $\nu : k \mapsto k'$ and that A is a K-algebra under $k \cdot a = k^\nu a$. One then verifies that the map $\chi : V \to A$ given by $v \mapsto \begin{pmatrix} v & v^\phi \\ 0 & v \end{pmatrix}$, is a K-linear map and so may be uniquely extended to a K-algebra map $\psi : K\{V\} \to A$.

Since T is generated as a K-algebra by V it is clear that for each $t \in T$ we have $t^{\psi} = \begin{pmatrix} t & t^{\mu} \\ 0 & t \end{pmatrix}$, $t^{\mu} \in T$, whence μ is the desired δ-derivation of $K\{V\}$.

We now approach these matters in a less sophisticated way. Let X be an arbitrary set, let $S{<}X{>}$ be the free semigroup with 1 on the set X, let K be a commutative ring with 1, and let $K{<}X{>}$ denote the free K-module with basis $S{<}X{>}$. Multiplication is defined in the obvious way by juxtaposition, and $K{<}X{>}$ is in fact a K-algebra. Now let P be any K-algebra and $\phi : X \to P$ any set mapping. Then ϕ may be uniquely extended to a K-algebra map $\psi : K{<}X{>} \to P$ by simply sending each basis element $s = x_1 x_2 \dots x_n$ to $x_1^{\phi} x_2^{\phi} \dots x_n^{\phi}$, $x_i \in X$. For this reason we call $K{<}X{>}$ the *free algebra on the set X over K.*

Let X be a set, let V be the free K-module with basis X' in one-one correspondence with X. The K-linear map $V \to K{<}X{>}$ given by $x' \mapsto x$ may be lifted to a K-algebra map $K\{V\} \to K{<}X{>}$, and conversely the set map $x \mapsto x'$ may be lifted to a K-algebra map $K{<}X{>} \to K\{V\}$. Thus $K\{V\} \cong K{<}X{>}$, and, identifying X and X', we may state:

Remark 1.2.4 *If V is a free K-module with basis X, then $K\{V\} = K{<}X{>}$.*

In view of Remark 1.2.4 the equivalent formulations of Corollaries 1.2.2 and 1.2.3 for $K{<}X{>}$ can now be stated without further proof.

Remark 1.2.5 *Let $K{<}X{>}$ be the free K-algebra in X over a commutative ring K and let P be a K-algebra with* 1. *Then:*

(a) If σ is an automorphism of K and $\phi : X \to P$ is a set map, then there is a unique σ-homomorphism $\psi : K{<}X{>} \to P$ extending ϕ and also a unique σ-antihomomorphism $\rho : K{<}X{>} \to P$ extending ϕ.

(b) If δ is a derivation of K, and $\phi : X \to K{<}X{>}$ is a set map, then there is a unique δ-derivation ψ of $K{<}X{>}$ extending ϕ.

Finally, suppose A and B are K-algebras. Then $A \otimes_K B$ becomes a K-algebra under multiplication given by

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$$

and its consequences.

Remark 1.2.6 *Let A, B, P be K-algebras and $\alpha : A \to P$, $\beta : B \to P$ K-algebra maps such that $[A^\alpha, B^\beta] = 0$. Then there is a unique K-algebra map $\gamma : A \otimes_K B \to P$ such that $(a \otimes b)^\gamma = a^\alpha b^\beta$.*

Remark 1.2.7 *Let A, B, P be K-algebras, let $\omega : K \to K$ be a ring homomorphism, and let $\alpha : A \to P$, $\beta : B \to P$ be ω-semilinear ring homomorphisms such that $[A^\alpha, B^\beta] = 0$. Then there is a unique ω-semilinear ring homomorphism $\gamma : A \otimes_K B \to P$ such that $(a \otimes b)^\gamma = a^\alpha b^\beta$.*

Proof. We consider P as a K-algebra P^* by defining $k \cdot p = k^\omega p$, $k \in K$, $p \in P$. Then $\alpha : A \to P^*$, $\beta : B \to P^*$ are K-algebra maps and so the K-algebra map given by Remark 1.2.6 is the required ω-semilinear ring homomorphism $\gamma : A \otimes_K B \to P$.

Remark 1.2.8 *Let A, B, P be K-algebras, let $\omega : K \to K$ be a ring homomorphism, and let $\alpha : A \to P$, $\beta : B \to P$ be ω-semilinear ring antihomomorphisms such that $[A^\alpha, B^\beta] = 0$. Then there is a unique ω-semilinear ring antihomomorphism $\gamma : A \otimes_K B \to P$ such that $(a \otimes b)^\gamma = a^\alpha b^\beta$.*

Proof. Let P° denote the opposite algebra of P, note that $\alpha : A \to P^\circ$, $\beta : B \to P^\circ$ are ω-semilinear ring homomorphisms such that $a^\alpha \circ b^\beta - b^\beta \circ a^\alpha = 0$, and apply Remark 1.2.7.

Remark 1.2.9 *Let A, B be K-algebras with* 1, *let $\rho : K \to K$ be a derivation, and let $\delta : A \to A$, $\mu : B \to B$ be ρ-derivations. Then there is a unique ρ-derivation $\tau : A \otimes B \to A \otimes B$ such that $(a \otimes b)^\tau = a^\delta \otimes b + a \otimes b^\mu$.*

Proof. We set $C = A \otimes_K B$, let R be the set of all matrices in $M_2(C)$ of the form $r = \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}$, $c, d \in C$, and let K' be the set of all matrices of the form $k' = \begin{pmatrix} k & k^\rho \\ 0 & k \end{pmatrix}$, $k \in K$, One readily checks that $K' \cong K$ via the map $\nu : k \mapsto k'$ and R is a K-algebra under $k \circ r = k^\nu r$. The mappings $\alpha : a \mapsto \begin{pmatrix} a \otimes 1 & a^\delta \otimes 1 \\ 0 & a \otimes 1 \end{pmatrix}$, $\beta : b \mapsto \begin{pmatrix} 1 \otimes b & 1 \otimes b^\mu \\ 0 & 1 \otimes b \end{pmatrix}$ are respectively K-algebra maps of A into R and B into R such that $[A^\alpha, B^\beta] = 0$. Consequently by Remark 1.2.6 there is a unique K-algebra map $\gamma : A \otimes B \to R$ such that $(a \otimes b)^\gamma = a^\alpha b^\beta$. Since $A \otimes B$ is generated by $A \otimes 1$ and $1 \otimes B$ it is clear that for $c \in C$, $c^\gamma = \begin{pmatrix} c & c^\tau \\ 0 & c \end{pmatrix}$, whence τ is the desired ρ-derivation of $A \otimes B$.

1.3 The Diamond Lemma

Our goal in this section is the Diamond Lemma, which is the main tool in our proof of the Poincaré-Birkhoff-Witt thorems. We note that the technique of composition for Lie algebras was introduced by A. I. Shirshov [273] in 1962 and further extended to the Composition (Diamond) Lemmas for Lie algebras and for associative algebras by L. A. Bokut ([56] and [57]) and by G. Bergman [52] (see also [58]).

Let $(Y, \leq)$ be a partially ordered set and let $\mathcal{E}(Y)$ be the set of all finite subsets of Y consisting of pairwise incomparable elements. For $U, V \in \mathcal{E}(Y)$ we define: $U \leq V$ if for all $u \in U$ there exists $v \in V$ such that $u \leq v$. We claim $(\mathcal{E}(Y), \leq)$ is a partially ordered set. Indeed, transitivity is clear. Next suppose $U \leq V$ and $V \leq U$ and let $u \in U$. If $u \notin V$ then $u < v$ for some $v \in V$ and from $v \leq u'$ for some $u' \in U$ we see that $u < u'$, contradicting the incomparability of the elements of U. Thus $U = V$ and we have shown $\leq$ is antisymmetric.

Lemma 1.3.1 *If* $(Y, \leq)$ *satisfies the DCC then* $(\mathcal{E}(Y), \leq)$ *also satisfies the DCC.*

Proof. Suppose $U_0 > U_1 > \dots U_n > \dots$ is an infinite descending chain in $\mathcal{E}(Y)$. Without loss of generality we may assume for each $n \geq 1$ there is an element $v_n \in U_n$ such that $v_n < w_{n-1}$ for some $w_{n-1} \in U_{n-1}$ (otherwise there would exist m such that $U_m \supset U_{m+1} \supset \dots$ is a infinite sequence of proper inclusions, in contradiction to the finiteness of U_m). If $v_k = v_n$ for some $k < n$ then we obtain the contradiction $v_k = v_n < w_{n-1} \leq u_k$ for some $u_k \in U_k$. Therefore the v_n's are distinct and so in particular $\bigcup_{n=1}^{\infty} U_n$ is infinite.

A *path* is a sequence $p = (u_0, u_1, \dots, u_n, \dots)$, $u_n \in U_n$ (which can be finite or infinite) such that $u_n \geq u_{n+1}$ for each n. Given $x \in U_n$ we say that p passes through x if $u_n = x$. For any finite sequence

$$u_{i_0}, u_{i_1}, \dots, u_{i_k}, \quad u_{i_j} \in U_{i_j}, \quad u_{i_j} \geq u_{i_{j+1}}, \quad i_0 < i_1 < \dots < i_k,$$

$P(u_{i_0}, u_{i_1}, \dots, u_{i_k})$ is that subset of $\bigcup_{n=1}^{\infty} U_n$ formed from all paths passing simultaneously through $u_{i_0}, u_{i_1}, \dots, u_{i_k}$. Since every element of $\bigcup_{n=1}^{\infty} U_n$ lies in some path, by the finiteness of U_0 we may choose $u_0 \in U_0$ such that $P(u_0)$ is infinite. Suppose some $P(u_{i_0}, u_{i_1}, \dots, u_{i_k})$ (as defined above) is infinite. Then there exists $x \in P(u_{i_0}, u_{i_1}, \dots, u_{i_k})$ such that $x \notin \bigcup_{j=0}^{i_k} U_j$, since $\bigcup_{j=0}^{i_k} U_j$ is finite. Thus $x \in U_m$, $m > i_k$ and so $x \leq u_{i_k}$. It follows that $u_{i_k} \notin U_m$ and accordingly there exists $u_m \in U_m$, $u_m < u_{i_k}$, such that $P(u_{i_0}, u_{i_1}, \dots, u_{i_k}, u_m)$ is infinite. Repeated application of the above process then produces an infinite sequence

$u_{i_0} > u_{i_1} > \ldots > u_{i_k} > \ldots$ in contradiction to $(Y, \leq)$ satisfying the *DCC*.

Let Φ be a commutative ring with 1 and let X be a set. Denote by $Y = S{<}X{>}$ the free semigroup (with 1) generated by X, and let $\Phi{<}X{>}$ be the free Φ-algebra (with 1) generated by X. Consider a subset $\Lambda \subseteq Y \times \Phi{<}X{>}$ of the Cartesian product of Y and $\Phi{<}X{>}$. For any $\sigma = (W_\sigma, f_\sigma) \in \Lambda$, $A, B \in Y$, denote by $R_{A\sigma B}$ the endomorphism of the Φ-module $\Phi{<}X{>}$ given by the rule:

$$R_{A\sigma B}(AW_\sigma B) = Af_\sigma B \quad \text{and}$$
$$R_{A\sigma B}(U) = U \quad \text{for} \quad U \neq AW_\sigma B,\ U \in S{<}X{>}\,.$$

We call this set Λ a *reduction system* and the Φ-endomorphisms $R_{A\sigma B} : \Phi{<}X{>} \to \Phi{<}X{>}$ are called *reductions*. We say that an element $f \in \Phi{<}X{>}$ is *irreducible* if f does not contain monomials of the form $AW_\sigma B$ where $A, B \in Y$ and $\sigma = (W_\sigma, f_\sigma)$. Clearly the subset $\Phi{<}X{>}_{irr}$ of all irreducible elements of $\Phi{<}X{>}$ is a Φ-submodule of the module $\Phi{<}X{>}$.

Lemma 1.3.2 *Let $L = S{<}X{>} \cap \Phi{<}X{>}_{irr}$. Then L is a Φ-basis of the module $\Phi{<}X{>}_{irr}$.*

Proof. Clearly, the elements of the set L are linearly independent over Φ. Suppose that $\Phi{<}X{>}_{irr} \neq \sum_{l \in L} \Phi l$. Let $h \in \Phi{<}X{>}_{irr} \setminus \sum_{l \in L} \Phi l$. Further let $h = \sum_i k_i u_i$, where $k_i \in \Phi$, $u_i \in S{<}X{>}$. Clearly $u_i \notin L$ for some i. Hence there exists a reduction $R_{A\sigma B}$ such that $R_{A\sigma B}(u_i) \neq u_i$. Since $R_{A\sigma B}(u_j) = u_j$ for all $j \neq i$, $R_{A\sigma B}(h) \neq h$ in contradiction with $h \in \Phi{<}X{>}_{irr}$. Thus $\Phi{<}X{>}_{irr} = \sum_{l \in L} \Phi l$.

Suppose that for $f \in \Phi{<}X{>}$ there exists a finite sequence $R_1, \ldots, R_n$ of reductions such that $R_n R_{n-1} \ldots R_1(f) \in \Phi{<}X{>}_{irr}$. The element $R_n R_{n-1} \ldots R_1(f)$ is said to be a *normal form* of f (in general an element $g \in \Phi{<}X{>}$ may have no normal form, several normal forms, or a unique normal form). Denote by $\Phi{<}X{>}_{red}$ the subset of all elements f of $\Phi{<}X{>}$ with a unique normal form $N(f)$ (possibly $\Phi{<}X{>}_{red}= 0$).

A collection (σ, τ, A, B, C) is said to be an *overlap ambiguity* if $A, B, C \in Y$, $\sigma, \tau \in \Lambda$, and $W_\sigma = AB$, $W_\tau = BC$. We shall say that the overlap ambiguity (σ, τ, A, B, C) is *resolvable* if there exist compositions of reductions R and R' such that $R(R_{\sigma C}(ABC)) = R'(R_{A\tau}(ABC))$.

A collection (σ, τ, A, B, C) is said to be an *inclusion ambiguity* if $A, B, C \in Y$, $\sigma, \tau \in \Lambda$, and $W_\sigma = B$, $W_\tau = ABC$. We shall say that the inclusion ambiguity (σ, τ, A, B, C) is *resolvable* if there exist compositions of reductions R and R' such that $R(R_{A\sigma C}(ABC)) = R'(R_\tau(ABC))$.

A partial ordering $\leq$ on the set $Y = S{<}X{>}$ is said to be a *semigroup ordering* if $B < B'$ with $B, B' \in Y$ implies $ABC < AB'C$ for all $A, C \in Y$. A partial ordering $\leq$ on the set $S{<}X{>}$ is said to be *compatible* with Λ if for any $\sigma \in \Lambda$ the element f_σ is a linear combination of monomials V with $V < W_\sigma$.

Denote by $I = I(\Lambda)$ the two-sided ideal of $\Phi{<}X{>}$ generated by the elements $W_\sigma - f_\sigma$, $\sigma \in \Lambda$. Clearly the Φ-module I is generated by the elements $A(W_\sigma - f_\sigma)B$, where $A, B \in Y, \sigma \in \Lambda$.

With reference to $(Y, \leq)$ above and to Lemma 1.3.1, we denote by $O(h) \in \mathcal{E}(Y)$ the set of all maximal monomials in $h \in \Phi{<}X{>}$.

Lemma 1.3.3 *Under the above notations suppose $(S{<}X{>}, \leq)$ satisfies the DCC, where $\leq$ is a semigroup partial order compatible with the reduction system Λ. Then:*

(a) *Every element $f \in \Phi{<}X{>}$ has a normal form (not necessarily unique).*

(b) *$\Phi{<}X{>}_{red}$ is a Φ-submodule of $\Phi{<}X{>}$ and the mapping $N : \Phi{<}X{>}_{red} \to \Phi{<}X{>}_{irr}$ is a Φ-module homomorphism.*

(c) *For any sequence R of reductions $R(f) - f \in I(\Lambda)$ for all $f \in \Phi{<}X{>}$.*

Proof. **(a)** Suppose the contrary. Then the set H of all elements of $\Phi{<}X{>}$ which can not be reduced to a normal form is not empty. By Lemma 1.3.1 it follows that in the set $\{O(g) \mid g \in H\}$ there exist minimal elements. Choose an element $h \in H$ such that $O(h)$ is minimal in $\{O(g) \mid g \in H\}$, and the number $|O(h)|$ is minimal possible. Let $h = \sum_u k_u u$, where $k_u \in \Phi$, $u \in S{<}X{>}$. We set $p = \sum_{u \in O(h)} k_u u$, $q = h - p$. Clearly $O(q) < O(p) = O(h)$. By our choice of the element h, there exists a sequence of reductions R such, that $R(q) \in \Phi{<}X{>}_{irr}$. Since the semigroup partial ordering $\leq$ is compatible with Λ and monomials in $O(p)$ are pairwise incomparable, for any reduction $R_{A\sigma B}$ we have that either $R_{A\sigma B}(p) = p$, or $O(R_{A\sigma B}(p)) < O(p)$. Hence either $R(p) = p$, or $O(R(p)) < O(p)$. By the choice of h, in the last case there exists a sequence of reductions R' such that $R'R(p) \in \Phi{<}X{>}_{irr}$. Since $R(q) \in \Phi{<}X{>}_{irr}$, $R'R(q) = R(q)$. Hence we obtain

$$R'R(h) = R'R(p) + R'R(q) = R'R(p) + R(q) \in \Phi{<}X{>}_{irr} .$$

By the choice of the element h this case is impossible. Therefore, $R(p) = p$. As $p \notin \Phi{<}X{>}_{irr}$, there exists a reduction $R_{A\sigma B}$ such that $R_{A\sigma B}(p) \neq p$. By the above this is impossible and so we have a contradiction. Thus any element of $\Phi < X >$ may be reduced to a normal form.

(b) Let $f, g \in \Phi{<}X{>}_{red}$, $\alpha, \beta \in \Phi$ and R any sequence of reductions. Since the element $R(f)$ has a normal form and this normal form is also a normal form of the element f, there exists a sequence of reductions R' such that $R'R(f) = N(f)$. Analogously, $R''R'R(g) = N(g)$ for some sequence of reductions R''. Hence we have

$$\begin{aligned} R''R'R(\alpha f + \beta g) &= \alpha R''(N(f)) + \beta N(g) \\ &= \alpha N(f) + \beta N(g) \in \Phi{<}X{>}_{irr} . \end{aligned}$$

Therefore, $\alpha N(f)+\beta N(g)$ is a normal form of elements $\alpha f+\beta g$ and $R(\alpha f+\beta g)$. Since R is an arbitrary sequence of reductions, the element $\alpha f+\beta g$ has a unique normal form. Thus $\alpha f+\beta g \in \Phi{<}X{>}_{red}$ and $N(\alpha f+\beta g)=\alpha N(f)+\beta N(g)$.

(c) Since $W_\sigma - f_\sigma \in I$ for all $\sigma \in \Lambda$, $R_{A\sigma B}(g)-g \in I$ for all $A, B \in S{<}X{>}$, $g \in \Phi{<}X{>}$. So $R(g)-g \in I$ for any sequence of reductions R.

Theorem 1.3.4 (Diamond Lemma) *(see [52] and [57]). Let Λ be a reduction system for the free associative Φ-algebra $\Phi{<}X{>}$ and $\leq$ be a semigroup partial ordering on $S{<}X{>}$ compatible with Λ and satisfying the descending chain condition. Then the following conditions are equivalent:*

(a) All ambiguities of Λ are resolvable;

(b) $\Phi{<}X{>}= \Phi{<}X{>}_{red}$, i.e. any element of $\Phi{<}X{>}$ has a unique normal form;

(c) $\Phi{<}X{>}= \Phi{<}X{>}_{irr} \oplus I(\Lambda)$.

If these conditions hold, then $\Phi{<}X{>}/I(\Lambda)$ may be identified with the Φ-module $\Phi{<}X{>}_{irr}$, which is a Φ-algebra under the multiplication $f \times g = N(fg)$.

Proof. Assume that **(c)** holds. Then $\Phi{<}X{>}= \Phi{<}X{>}_{irr} \oplus I$, where $I = I(\Lambda)$. Let $f \in \Phi{<}X{>}$. By Lemma 1.3.3, the element f has a normal form. Suppose that it has two different normal forms $g, g' \in \Phi{<}X{>}_{irr}$. Since $g-f \in I$ and $g'-f \in I$, $g-g' \in \Phi{<}X{>}_{irr} \cap I = 0$, and we have a contradiction. Thus the element f has the unique normal form, $\Phi{<}X{>}= \Phi{<}X{>}_{red}$ and **(c)** implies **(b)**.

Suppose that **(b)** holds. Then N is a projection of the Φ-module $\Phi{<}X{>}$ onto $\Phi{<}X{>}_{irr}$. Since $N(g)-g \in I$, $\ker N \subseteq I$. As elements of $\Phi{<}X{>}= \Phi{<}X{>}_{red}$ have a unique normal form,

$$N(A(W_\sigma - f_\sigma)B) = N(AW_\sigma B) - N(Af_\sigma B) = 0$$

for all $A, B \in S{<}X{>}$, $\sigma \in \Lambda$. Furthermore, the Φ-submodule I is generated by the elements of the form $A(W_\sigma - f_\sigma)B$. Therefore, ker $N \supseteq I$. Hence ker $N = I$ and $\Phi{<}X{>} = \Phi{<}X{>}_{irr} \oplus I$. Thus, conditions **(b)** and **(c)** are equivalent.

Obviously, **(b)** implies **(a)**. We show that **(a)** implies **(b)**. By Lemma 1.3.3, $\Phi{<}X{>}_{red}$ is a Φ-submodule and the normal form mapping $N : \Phi{<}X{>}_{red} \to \Phi{<}X{>}_{irr}$ is a homomorphism of Φ-modules. It is enough to prove that $S{<}X{>} \subseteq \Phi{<}X{>}_{red}$.

Assume that $S{<}X{>} \setminus \Phi{<}X{>}_{red} \neq \emptyset$. Let w be a minimal element of the set $S{<}X{>} \setminus \Phi{<}X{>}_{red}$. Furthermore let $R_{U\sigma V'}$ and $R_{U'\tau V}$ be two different reductions such that $R_{U\sigma V'}(w) \neq R_{U'\tau V}(w)$. Clearly, $UW_\sigma V' = w = U'W_\tau V$. By the choice of the element w, $R_{U\sigma V'}(w) \in \Phi{<}X{>}_{red}$ and $R_{U'\sigma V}(w) \in \Phi{<}X{>}_{red}$. It is enough to prove that $N(R_{U\sigma V'}(w)) = N(R_{U'\tau V}(w))$. Without loss of generality one can assume that $U' = UA$ for some $A \in S{<}X{>}$. Consider three possible cases.

Case 1. We have an overlap ambiguity $w = UABCV$, $W_\sigma = AB$, $W_\tau = BC$, $V' = CV$, $U' = UA$. By **(a)** this ambiguity is resolvable, i.e. the elements $f_\sigma C$ and Af_τ can be reduced to one and the same element f. Therefore the elements $R_{U\sigma V'}(w) = Uf_\sigma CV$, $R_{U'\tau V}(w) = UAf_\tau V$ can be reduced to the element $g = UfV$.

Case 2. We have an inclusion ambiguity $w = UABCV'$, $W_\sigma = ABC$, $W_\tau = B$, $V = CV'$, $U' = UA$. By analogy with the first case, one can show that the elements $R_{U\sigma V'}(w) = Uf_\sigma V$ and $R_{U'\tau V}(w) = UAf_\tau CV$ can be reduced to one and the same element.

Case 3. The subwords W_σ and W_τ are disjoint in w (i.e. $w = UW_\sigma BW_\tau V$, $U' = UW_\sigma B$, $V' = BW_\tau V$). Then

$$R_{U\sigma V'}(w) = Uf_\sigma BW_\tau V \quad \text{and} \quad R_{U'\tau V}(w) = UW_\sigma Bf_\tau V.$$

For any $v = x_1x_2\ldots x_k \in S{<}X{>}$, where $x_1, x_2, \ldots, x_k \in X$, we set $l(v) = k$. Without loss of generality we may assume that

$$f_\sigma = \sum_{i=1}^{m} \alpha_i p_i \quad \text{and} \quad f_\tau = \sum_{j=1}^{n} \beta_j q_j, \quad \text{where}$$

$$\begin{aligned}&\alpha_i, \beta_j \in \Phi,\ p_i, q_j \in S{<}X{>},\\ &l(p_i) \leq l(p_s), \quad p_i \neq p_s \quad \text{for all} \quad 1 \leq i < s \leq m, \quad \text{and}\\ &l(q_j) \leq l(q_t), \quad q_j \neq q_t \quad \text{for all} \quad 1 \leq j < t \leq n.\end{aligned}$$

We claim that

$$R_{Up_mB_TV} R_{Up_{m-1}B_TV} \dots R_{Up_1B_TV}(Uf_\sigma BW_\tau V) = Uf_\sigma Bf_\tau V.$$

Since $Uf_\sigma BW_\tau V = \sum_{i=1}^m \alpha_i Up_i BW_\tau V$, it is enough to prove that

$$R_{Up_mB_TV} R_{Up_{m-1}B_TV} \dots R_{Up_1B_TV}(Up_iBW_\tau V) = Up_iBf_\tau V$$

for all $1 \leq i \leq m$. Note that

$$\begin{aligned}&R_{Up_iB_TV} R_{Up_{i-1}B_TV} \dots R_{Up_1B_TV}(Up_iBW_\tau V) =\\ &R_{Up_iB_TV}(Up_iBW_\tau V) = Up_iBf_\tau V.\end{aligned}$$

So it is enough to prove that

$$R_{Up_sB_TV}(Up_iBf_\tau V) = Up_iBf_\tau V$$

for all $1 \leq i < s \leq m$. As $Up_iBf_\tau V = \sum_{j=1}^n \beta_j Up_iBq_jV$, we have to prove that

$$R_{Up_sB_TV}(Up_iBq_jV) = Up_iBq_jV$$

for all $1 \leq j \leq n$ and $1 \leq i < s \leq m$. Suppose the contrary. Then $Up_sBW_\tau V = Up_iBq_jV$. Hence $p_sBW_\tau = p_iBq_j$. Since $l(p_s) \geq l(p_i)$ and $p_s \neq p_i$, $l(p_s) > l(p_i)$. Taking into account that

$$l(p_sBW_\tau) = l(p_s) + l(B) + l(W_\tau) = l(p_i) + l(B) + l(q_j),$$

we have that $l(W_\tau) < l(q_j)$. That is to say $q_j = DW_\tau$ for some $1 \neq D \in S{<}X{>}$. Since the partial ordering $\leq$ of $S{<}X{>}$ is compatible with the reduction system Λ, $DW_\tau = q_j < W_\tau$. As this ordering is a semigroup one, $D^{n+1}W_\tau < D^nW_\tau$ for all

$n \geq 0$ which is a contradiction to the descending chain condition. Therefore

$$R_{Up_mBTV}R_{Up_{m-1}BTV}\dots R_{Up_1BTV}(Uf_\sigma BW_\tau V) = Uf_\sigma Bf_\tau V.$$

Analogously $R(UW_\sigma Bf_\tau V) = Uf_\sigma Bf_\tau V$ for some sequence of reductions R. That is to say elements $R_{U\sigma V'}(w)$ and $R_{U'\tau V}(w)$ are reduced to one and the same element.

Therefore in all cases it follows from

$$R_{U\sigma V'}(w), R_{U'\tau V}(w) \in \Phi{<}X{>}_{red}$$

that $N(R_{U\sigma V'}(w)) = N(R_{U'\tau V}(w))$. Thus the element w has a unique normal form and we have a contradiction.

We close this section with the famous Amitsur-Levitski Theorem [9]. The proof presented here is very simple and is due to S. Rosset [254]. Let X be an infinite set, $\mathcal{Z}$ the ring of integers, Q the field of rational numbers and $\mathcal{Z}{<}X{>}$ the free algebra over $\mathcal{Z}$ generated by X. Further let $n > 0$ be a natural number, S_n the symmetric group of order n and $\epsilon(\sigma)$ the sign of the permutation $\sigma \in S_n$. We set

$$St_n(x_1, x_2, \dots, x_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(n)}$$

where $x_1, x_2, \dots, x_n \in X$ are distinct variables and we will call St_n *the standard polynomial* of degree n.

Theorem 1.3.5 (Amitsur-Levitski) *Let R be a commutative ring, $n > 0$ a natural number and $M_n(R)$ the $n \times n$-matrix ring over R. Then for all $A_1, \dots, A_{2n} \in M_n(R)$*

$$St_{2n}(A_1, A_2, \dots, A_{2n}) = 0$$

(i.e., St_{2n} is a polynomial identity of $M_n(R)$).

We start with the following easy remarks (here $tr(A)$ is the trace of the matrix $A \in M_n(R)$)

Remark 1.3.6 *Let R be a commutative algebra over Q and $A \in M_n(K)$. Suppose that $tr(A^i) = 0$ for all $i > 0$. Then $A^n = 0$.*

Proof. Adjoining (if it is necessary) an identity element to R, we can assume that R has an identity. Consider the polynomial ring $K = Q[x_{ij} \mid 1 \leq i,j \leq n]$ and let $U = (x_{ij})_{i,j=1}^n \in M_n(K)$. The Newton formula on symmetric polynomials shows that the coefficients of the characteristic polynomial $\chi_U(t) = t^n + u_1 t^{n-1} + \ldots + u_n$ of U are polynomials with rational coefficients (and with zero constant terms) in the traces $tr(U^i)$, $i = 1, 2, \ldots, n$. Clearly there exists a Q-algebra map $\phi : K \to R$ such that for its canonical extension $\Phi : M_n(K) \to M_n(R)$ we have $\Phi(U) = A$. Then $\phi(u_i) = 0$ for all $i = 1, 2, \ldots, n$ and

$$A^n = \Phi(U^n) + \phi(u_1)\Phi(U^{n-1}) + \ldots + \phi(u_n) = \Phi(\chi_U(U)) = 0.$$

Remark 1.3.7 *If r is an even natural number, then*

$$tr(St_r(A_1, A_2, \ldots, A_r)) = 0$$

for all $A_1, A_2, \ldots, A_r \in M_n(R)$.

Proof. It is well-known that $tr(AB) = tr(BA)$. Let $\tau = (1, 2, \ldots, r) \in S_r$ be a cycle and let A_r be the alternating subgroup of S_r. Clearly $S_r = A_r \cup A_r\tau$ and $\epsilon(\sigma\tau) = -1$ for all $\sigma \in A_r$. Further we have

$$\begin{aligned} tr(A_{\sigma(1)}A_{\sigma(2)} \ldots A_{\sigma(r)}) &= tr(A_{\sigma(2)}A_{\sigma(3)} \ldots A_{\sigma(r)}A_{\sigma(1)}) \\ &= tr(A_{\sigma\tau(1)}A_{\sigma\tau(2)} \ldots A_{\sigma\tau(r)}) \end{aligned}$$

for all $\sigma \in A_r$ and so

$$\begin{aligned} tr(St_r(A_1, A_2, \ldots, A_r)) &= \sum_{\sigma \in A_r} tr(A_{\sigma(1)} A_{\sigma(2)} \ldots A_{\sigma(r)}) \\ &\quad - \sum_{\sigma \in A_r} tr(A_{\sigma\tau(1)} A_{\sigma\tau(2)} \ldots A_{\sigma\tau(r)}) \\ &= 0. \end{aligned}$$

The proof is complete.

Let $K = Q[x_{ijk} \mid 1 \leq i, j \leq n,\ 1 \leq k \leq 2n]$ be the polynomial ring in x_{ijk} over Q and $B_k = (x_{ijk})_{i,j=1}^n \in M_n(K)$. Consider the free algebra $F = K{<}Y{>}$ where $Y = \{y_1, \ldots, y_{2n}\}$. Letting I denote the ideal of F generated by all elements of the form $y_i y_j + y_j y_i$, we set

$$D = F/I,\ e_i = y_i + I,\ i = 1, 2, \ldots, 2n.$$

The reduction system for F consisting of all pairs $(y_j y_i, -y_i y_j)$, $i \leq j$, is clearly compatible with the usual ordering of monomials (i.e., first by length and then lexicographic). It then follows easily from the Diamond Lemma that 1 and all elements $e_{i_1} e_{i_2} \ldots e_{i_k}$, where $k \leq n$ and $i_1 < i_2 < \ldots < i_k$, form a basis of the K-module D. Clearly $e_{i_1} e_{i_2} \ldots e_{i_k} \in Z(D) = C$ if k is even where $Z(D)$ is the center of D. Noting that $M_n(K) \subseteq M_n(C) \subseteq M_n(D)$, we set $B = B_1 e_1 + B_2 e_2 + \ldots + B_{2n} e_{2n} \in M_n(D)$. Obviously

$$B^k = \sum_{i_1 < i_2 < \ldots < i_k} St_k(B_{i_1}, B_{i_2}, \ldots, B_{i_k}) e_{i_1} e_{i_2} \ldots e_{i_k}. \tag{1.1}$$

In particular, $B^k = 0$ for $k > 2n$ and

$$B^{2n} = St_{2n}(B_1, B_2, \ldots, B_{2n}) e_1 e_2 \ldots e_{2n}$$

For any natural number $r > 0$ we have $B^{2r} = (B^2)^r \in M_n(C)$. Now from (1.1) and Remark 1.3.7 it follows that

$$tr\left(\left(B^2\right)^r\right) = 0$$

and so $B^{2n} = (B^2)^n = 0$ by Remark 1.3.6. Therefore

$$St_{2n}(B_1, B_2, \dots, B_{2n}) = 0.$$

Consider the subring $L = \mathcal{Z}[x_{ijk} \mid 1 \le i, j \le n,\ 1 \le k \le 2n] \subseteq K$. Clearly $B_i \in M_n(L) \subseteq M_n(K)$. Since there exists a ring homomorphism $\phi : L \to R$ such that for its canonical extension $\Phi : M_n(L) \to M_n(R)$ we have $\Phi(B_i) = A_i$ for all $1 \le i \le 2n$, we conclude that $St_{2n}(A_1, A_2, \dots, A_{2n}) = 0$, and the proof of Amitsur-Levitski Theorem is complete.

1.4 Coproducts

The notion of a coproduct is fundamental to this book since (as we shall see in Chapter 6) it forms the "home" in which "generalized identities" live.

Let A_1 and A_2 be algebras with 1 over a commutative ring K. Then a K-algebra A with 1 is a *coproduct of* A_1 *and* A_2 *over* K if:

(i) *There exist* K*-algebra homomorphisms* $\alpha : A_1 \to A$ *and* $\beta : A_2 \to A$ *such that* $A_1^\alpha \cup A_2^\beta$ *generates* A *as a* K*-algebra.*

(ii) *For any* K*-algebra* P *with* 1 *and homomorphisms* $\sigma : A_1 \to P$ *and* $\tau : A_2 \to P$ *there exists a homomorphism* $\phi : A \to P$ *such that* $\alpha\phi = \sigma$ *and* $\beta\phi = \tau$, i.e., *the diagram*

$$\begin{tikzcd}
A_1 \arrow[r, "\alpha"] \arrow[dr, "\sigma"'] & A \arrow[d, dashed, "\phi"'] & A_2 \arrow[l, "\beta"'] \arrow[dl, "\tau"] \\
& P &
\end{tikzcd}$$

can always be completed.

It is immediate from (i) and (ii) that ϕ is uniquely determined by σ and τ. It is also easy to see that if A and A' are any two coproducts of A_1 and A_2 over K then A and A' are isomorphic via isomorphisms ϕ and ϕ' as indicated in the following self-explanatory diagram:

$$\begin{tikzcd}
A_1 \arrow[r, "\alpha"] \arrow[dr, "\alpha'"'] & A \arrow[d, shift right, "\phi"'] & A_2 \arrow[l, "\beta"'] \arrow[dl, "\beta'"] \\
& A' \arrow[u, shift right, "\phi'"'] &
\end{tikzcd}$$

Indeed, for the K-algebra maps ϕ and ϕ' one simply checks that $\phi\phi'$ (resp. $\phi'\phi$) acts as the identity map on the generators $A_1^\alpha \cup A_2^\beta$ of A (resp. $A_1^{\alpha'} \cup A_2^{\beta'}$ of A').

We next show the existence of the coproduct of A_1 and A_2 over K by the following natural (if somewhat cumbersome) construction. The idea is to first ”overshoot the mark” by finding an algebra generated by A_1 and A_2 (thus guaranteeing **(i)**) and then to factor out an appropriate ideal of this algebra (thus guaranteeing **(ii)**). Let

$$T = A_1 \oplus A_2 \oplus A_1 \otimes A_1 \oplus A_1 \otimes A_2 \oplus A_2 \otimes A_1 \oplus \ldots$$

be the tensor algebra of A_1 and A_2 (as defined in section 1.2), and let I be the ideal of T generated by all elements of the form

$$a_1 \otimes b_1 - a_1 b_1; \quad a_2 \otimes b_2 - a_2 b_2; \quad 1_{A_1} - 1_{A_2} \qquad (1.2)$$

where $a_1, b_1 \in A_1$, $a_2, b_2 \in A_2$. We claim that $A = T/I$ is a coproduct of A_1 and A_2 over K. Let α_0 and β_0 be the respective inclusion maps $\alpha_0 : A_1 \to T$, $\beta_0 : A_2 \to T$, and, letting ν denote the natural homomorphism of T onto T/I, we define $\alpha_1 : A_1 \to A$ by $\alpha_1 = \alpha_0 \nu$ and $\beta_1 : A_2 \to A$ by $\beta_1 = \beta_0 \nu$. Property **(i)** is then clear. Now consider homomorphisms $\sigma : A_1 \to P$, $\tau : A_2 \to P$, P a K-algebra. We first complete the diagram

$$\begin{tikzcd}
A_1 \arrow[r, "\alpha_0"] \arrow[dr, "\sigma"'] & T \arrow[d, dashed, "\phi_0"'] & A_2 \arrow[l, "\beta_0"'] \arrow[dl, "\tau"] \\
& P &
\end{tikzcd}$$

Indeed, it suffices to define ϕ_0 on each direct summand $T_1 \otimes T_2 \otimes \ldots \otimes T_m$ of T, where each T_i is either A_1 or A_2, and then extend by linearity. The map $\chi : T_1 \otimes T_2 \otimes \ldots \otimes T_m \to P$ given by $t_1 \otimes t_2 \otimes \ldots \otimes t_m \mapsto t_1^{\rho} t_2^{\rho} \ldots t_m^{\rho}$ (where $\rho = \sigma$ or $\rho = \tau$ depending on whether $t_i \in A_1$ or $t_i \in A_2$) is already K-linear, and from the nature of multiplication in T it is easy to see that ϕ_0 is a K-algebra homomorphism. Furthermore, by applying ϕ_0 to the generators (1.2) it is clear that ϕ_0 maps I to 0. As a result ϕ_0 may by lifted to a K-algebra homomorphism $\phi : T/I \to P$ by defining $(\bar{t})^{\phi} = t^{\phi_0}$, $\quad \bar{t} = t + I$, $\quad t \in T$. The commutativity of the above diagram then yields the commutativity of

$$\begin{tikzcd}
A_1 \arrow[r, "\alpha_1"] \arrow[dr, "\sigma"'] & A \arrow[d, "\phi_0"'] & A_2 \arrow[l, "\beta_1"'] \arrow[dl, "\tau"] \\
& P &
\end{tikzcd}$$

which shows that property **(ii)** holds.

The existence and uniqueness of a coproduct of A_1 and A_2 having been established, we now refer to *the* coproduct of A_1 and A_2 and denote it by $A_1 \coprod_K A_2$.

In general $A_1^{\alpha} \cap A_2^{\beta}$ may properly contain K. For instance, the reader may check that $Q \coprod_Z Q$ provides such an example. Furthermore the maps α and β need not be injections. For example, $Q \coprod_Z Z_2 = 0$. To alleviate these unwanted occurrences we make the following

Remark 1.4.1 *Let A_1 and A_2 be K-algebras with* 1 *such that*

$$K \quad \text{is a} \quad K-\text{direct summand of both} \quad A_1 \quad \text{and} \quad A_2. \qquad (1.3)$$

Then:
(*a*) $A_1^\alpha \cap A_2^\beta = K$;
(*b*) α *and* β *are injections.*

Proof. Consider the commutative diagram

$$\begin{tikzcd}
A_1 \arrow[r, "\alpha"] \arrow[dr, "\sigma"'] & A_1 \coprod A_2 \arrow[d, "\phi"] & A_2 \arrow[l, "\beta"'] \arrow[dl, "\tau"] \\
& A_1 \otimes A_2 &
\end{tikzcd}$$

where $\sigma(a_1) = a_1 \otimes 1$ and $\tau(a_2) = 1 \otimes a_2$ for all $a_1 \in A_1$, $a_2 \in A_2$. If $a_1^\alpha = a_2^\beta$ then $a_1 \otimes 1 = 1 \otimes a_2$. Let $\pi : A_1 \to K$ be the projection of A_1 onto the direct summand K. Clearly the mapping $A_1 \times A_2 \to A_2$ given by the rule $(b_1, b_2) \mapsto \pi(b_1)b_2$ is balanced. Hence it may be lifted to a K-module homomorphism $\psi : A_1 \otimes A_2 \to A_2$. Now we have

$$a_2 = \pi(1_{A_1})a_2 = \psi(1 \otimes a_2) = \psi(a_1 \otimes 1) = \pi(a_1)1_{A_2} \in K.$$

Analogously one can show $a_1 \in K$ and so (a) is proved. If $a_2 \in \ker \beta$ then $1 \otimes a_2 = 0$ and so $a_2 = \psi(1 \otimes a_2) = 0$. Thus β (and similarly α) is an injection, whence (b) has been proved.

In particular (1.3) is satisfied in case K is a field (this situation will occur when we study prime rings) or more generally in case K is commutative von Neumann regular selfinjective (this situation will occur when we study semiprime rings). With this motivation in mind we will henceforth assume that all K-algebras satisfy condition (1.3).

In view of Remark 1.4.1 we are now entitled to suppress α and β and to assume that A_1 and A_2 are in fact subalgebras of $A_1 \coprod A_2$, with $A_1 \cap A_2 = K$.

Under certain conditions it is possible to simultaneously lift homomorphisms, anti-homomorphisms, and derivations of A_1 and A_2 to $A_1 \coprod A_2$ even if these mappings are not K-linear. These considerations will be important ones in the sequel, and we proceed to indicate how they may be accomplished.

Remark 1.4.2 *Let A_1, A_2, P be K-algebras, let $\omega : K \to K$ be a ring homomorphism, and let $\sigma : A_1 \to P, \quad \tau : A_2 \to P$ be ω-semilinear ring homomorphisms. Then there is an ω-semilinear ring homomorphism $\phi : A_1 \coprod A_2 \to P$ simultaneously extending σ and τ.*

Proof. We consider P as a K-algebra P^* by defining $k \cdot p = k^\omega p, \quad k \in K, p \in P$. Then $\sigma : A_1 \to P^*$, $\tau : A_2 \to P^*$ are K-algebra maps and so by **(ii)** may be extended to K-linear map $\phi : A_1 \coprod A_2 \to P^*$, i.e., an ω-semilinear ring homomorphism $\phi : A_1 \coprod A_2 \to P$.

Remark 1.4.3 *Let A_1, A_2, P be K-algebras, let $\omega : K \to K$ be a ring homomorphism, and let $\sigma : A_1 \to P, \quad \tau : A_2 \to P$ be ω-semilinear ring anti-homomorphisms. Then there is an ω-semilinear ring anti-homomorphism $\phi : A_1 \coprod A_2 \to P$ simultaneously extending σ and τ.*

Proof. Let P° denote the opposite algebra of P, note that $\sigma : A_1 \to P^\circ, \quad \tau : A_2 \to P^\circ$ are ω-semilinear ring homomorphisms, and apply Remark 1.4.2.

Remark 1.4.4 *Let A_1 and A_2 be K-algebras, and let $\rho : K \to K, \quad \delta : A_1 \to A_1, \quad \mu : A_2 \to A_2$ be derivations (not necessarily*

K-linear) such that δ and μ agree with ρ on K. Then δ and μ can be simultaneously extended to a derivation $\psi : A_1 \coprod A_2 \to A_1 \coprod A_2$.

Proof. We set $A = A_1 \coprod A_2$, let R be the set of all matrices in $M_2(A)$ of the form $r = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, $a, b \in A$, and let K' be the set of all matrices of the form $k' = \begin{pmatrix} k & k^\rho \\ 0 & k \end{pmatrix}$, $k, k \in K$. One readily checks that K' is isomorphic to K via the mapping $\nu : k \mapsto k'$ and that R is a K-algebra under $k \cdot r = k^\nu r$. The mappings $\sigma : a_1 \mapsto \begin{pmatrix} a_1 & a_1^\delta \\ 0 & a_1 \end{pmatrix}$ and $\tau : a_2 \mapsto \begin{pmatrix} a_2 & a_2^\mu \\ 0 & a_2 \end{pmatrix}$ are respectively K-algebra maps of A_1 into R and of A_2 into R. Consequently σ and τ may be simultaneously extended to a unique K-algebra map $\phi : A \to R$. Since A is generated by A_1 and A_2 it is clear that, for $a \in A$, $a^\phi = \begin{pmatrix} a & a^\psi \\ 0 & a \end{pmatrix}$, whence ψ is the desired derivation of $A_1 \coprod A_2$.

As an application of the Diamond Lemma we prove the useful

Lemma 1.4.5 *Let A_1 and A_2 be algebras with 1 over K with respective K-bases $\{1\} \cup B_1$ and $\{1\} \cup B_2$. Then $\{1\} \cup M$ is a K-basis of $A_1 \coprod A_2$, where M is the set of all alternating monomials from B_1 and B_2.*

Proof. We outline the proof, leaving some details for the reader to fill in. Writing $B_1 = \{a_i\}$ we have for each i, k

$$a_i a_k = \alpha_{ik} 1 + \sum_{a_p \in B_1} \alpha_{ikp} a_p \tag{1.4}$$

Repeated use of (1.4) applied to $(a_i a_k) a_m = a_i (a_k a_m)$ then produces

$$\sum_p \alpha_{ikp} \alpha_{pmr} = \sum_p \alpha_{ipr} \alpha_{kmp} \tag{1.5}$$

for each i, k, m, r. A similar set of equations results from considering $B_2 = \{b_j\}$ and writing

$$b_j b_l = \beta_{jl} 1 + \sum_q \beta_{jlq} b_q$$

Letting $X = \{x_i\}$ and $Y = \{y_j\}$ be sets of indeterminates corresponding respectively to B_1 and B_2, we form the free algebra $K{<}X \cup Y{>}$ and let $\leq$ be the partial ordering on the free semigroup $S < X \cup Y >$ determined by the length of a monomial. Clearly $\leq$ is a semigroup partial ordering which satisfies the descending chain condition. The reduction system Λ of all pairs

$$\sigma_{ik} = (x_i x_k, \alpha_{ik} 1 + \sum_{x_p \in X} \alpha_{ikp} x_p), \quad \tau_{jl} = (y_j y_l, \beta_{jl} 1 + \sum_{y_q \in Y} \beta_{jlq} y_q)$$

is obviously compatible with $\leq$. It is easy to see that the only types of ambiguities which occur are overlapping ones of the form

$$(\sigma_{ik}, \sigma_{km}, x_i, x_k, x_m) \quad \text{or} \quad (\tau_{jl}, \tau_{ln}, y_j, y_l, y_n) \tag{1.6}$$

To resolve the first of these (the second is similarly resolved) we have only to note that

$$\prod_p R_{\sigma_{pm}} R_{\sigma_{ik} x_m}(x_i x_k x_m) = \prod_p R_{\sigma_{ip}} R_{x_i \sigma_{km}}(x_i x_k x_m)$$

in view of (1.5). By Lemma 1.3.2, $\{1\} \cup N$ is a K-basis of $K{<}X \cup Y{>}_{irr}$, where N is the set of all alternating monomials of X and Y. Therefore by Theorem 1.3.4(c) the cosets determined by $\{1\} \cup N$ form a K-basis of $K < X \cup Y > /I(\Lambda)$. The K-module mapping of A_1 into $K{<}X \cup Y{>}/I(\Lambda)$ given by $1_{A_1} \mapsto 1 + I(\Lambda)$, $a_i \mapsto x_i + I(\Lambda)$ is in fact a K-algebra map because of (1.4) and (1.6). Similarly $1_{A_2} \mapsto 1 + I(\Lambda)$, $b_j \mapsto y_j + I(\Lambda)$ yields a K-algebra map of A_2 into $K{<}X \cup Y{>}$, and these two maps can be extended simultaneously to a K-algebra map $\phi : A_1 \coprod A_2 \to$

$K{<}X \cup Y{>}/I(\Lambda)$. On the other hand the K-algebra map from $K{<}X \cup Y{>}$ to $A_1 \coprod A_2$ via $1 \mapsto 1$, $x_i \mapsto a_i$, $y_j \mapsto b_j$ sends $I(\Lambda)$ to 0 (because of (1.6)) and thus induces a K-algebra map $\psi : K{<}X \cup Y{>}/I(\Lambda) \to A_1 \coprod A_2$. Clearly ϕ and ψ are inverses of each other and thus $A_1 \coprod A_2 \cong K{<}X \cup Y{>}/I(\Lambda)$, whence $\{1\} \cup M$ is a K-basis of $A_1 \coprod A_2$.

In continuing our analysis of $A = A_1 \coprod A_2$ we assume for the remainder of this section that K is a field. This assures the existence of respective K-bases $\{1\} \cup B_1$ and $\{1\} \cup B_2$ for A_1 and A_2, and hence the basis $\{1\} \cup M$ for A as given by Lemma 1.4.5. The treatment we are embarking upon stems from a series of papers of P.M. Cohn ([94],[95],[96]) and we will freely borrow some terminology and portions of his account. We will make use of these matters in a later chapter, but in any case we feel this development is of independent interest.

A has a filtration given by $H^{-1} = 0$, $H^0 = K$, $H^1 = A_1 + A_2$, $H^n = \sum A_{i_1} A_{i_2} \ldots A_{i_n}$, $n = 1, 2, \ldots$. For any subscript $i = 1, 2$ let us agree to the convention that $i' = 2$ if $i = 1$ and $i' = 1$ if $i = 2$, and also to the convention that $A_i = A_1$ if i is odd and $A_i = A_2$ if i is even. We will express the fact that an element a of H^n actually lies in H^{n-1} by saying that $a \equiv 0\ (mod H^{n-1})$ or simply $a \equiv 0$ if the context is clear. For $i = 1, 2$ we set $H^n_{ij} = A_i A_{i+1} \ldots A_{i+n-1}$, where $j = i'$ if n is even and $j = i$ if n is odd. It is easy to see that $H^n_{ij} \supseteq H^{n-1}$, $H^n_{ij} H^m_{j'k} = H^{m+n}_{ik}$, and $H^n = H^n_{ij} + H^n_{i'j'}$. We denote the factor spaces H^n/H^{n-1} and H^n_{ij}/H^{n-1} by $\overline{H^n}$ and $\overline{H^n_{ij}}$ respectively. With the aid of Lemma 1.4.5 we are able to show the following

Lemma 1.4.6 *(a)* $\overline{H^n} = \overline{H^n_{ij}} \oplus \overline{H^n_{i'j'}}$ *(i.e., the decomposition of* $H^n = H^n_{ij} + H^n_{i'j'}$ *is unique modulo* H^{n-1}*).*

(b) $\overline{H^n_{ij}} \otimes \overline{H^m_{j'k}} \cong \overline{H^{m+n}_{ik}}$ *via the mapping* $\bar{u} \otimes \bar{v} \mapsto \overline{uv}$.

Proof. If $\{1\} \cup M$ is the basis of A given by Lemma 1.4.5, we let M^n be the subset of all elements of M of length n, and for

$i = 1, 2$ we let M_i^n be the subset of all elements of M^n whose left hand factors lie in B_i. Clearly $\{1\} \cup M^n$ is a K-basis of H^n and $\overline{M_i^n}$ is a K-basis of $\overline{H_{ij}^n}$. It follows that $H_{ij}^n \cap H_{i'j'}^n = H^{n-1}$ and so **(a)** is proved. To prove **(b)** we first note that the mapping $\phi : \overline{H_{ij}^n} \otimes \overline{H_{j'k}^m} \to \overline{H_{ik}^{m+n}}$ given by $\bar{u} \otimes \bar{v} \mapsto \overline{uv}$, $u \in H_{ij}^n$, $v \in H_{i'j'}^n$, is a well-defined surjective K-linear map. Then the elements $\{\overline{x_p} \otimes \overline{y_q} \mid x_p \in M_i^n,\ y_q \in M_{j'}^n\}$ are a K-basis of $\overline{H_{ij}^n} \otimes \overline{H_{j'k}^m}$, whose images $\overline{x_p y_q}$ under ϕ are precisely the elements of $\overline{M_i^{n+m}}$. It follows that ϕ is injective and the proof of **(b)** is complete.

The *height* $|a|$ of an element $a \in A$ is defined as follows: $|a| = n$ if $a \neq 0$, $a \in H^n$, $a \notin H^{n-1}$ and $|a| = -\infty$ if $a = 0$. The elements of H_{ij}^n which are of height n (i.e., which do not lie in H^{n-1}) are called (i, j)-*pure*. Elements of height $n \geq 1$ which are not (i, j)-pure for some i, j are called 0-*pure*. We shall frequently use the suggestive notation a_{ij} for an element of H_{ij}^n.

Remark 1.4.7 *Let $w \in H_{ij}^m$, $u \in H_{ik}^n$, $m \geq n$, and $u \not\equiv 0$ (mod H^{n-1}). Then there exist elements $u = u_1, u_2, \ldots, u_q \in H_{ik}^n$ which are independent modulo H^{n-1} and elements $v_1, \ldots, v_q \in H_{k'j}^{m-n}$ such that $w \equiv \sum_{p=1}^q u_p v_p$ (modH^{m-1}).*

Proof. Extend u to a basis of H_{ik}^n (*mod*H^{n-1}) and use the fact that $H_{ij}^m = H_{ik}^n H_{k'j}^{m-n}$.

Remark 1.4.8 *Let elements $u_1, \ldots, u_q \in H_{ij}^n$ be independent (modH^{n-1}), let $v_1, \ldots, v_q \in H_{j'k}^m$ and suppose $\sum_{p=1}^q u_p v_p \equiv 0$ (modH^{n+m-1}). Then $v_p \equiv 0$ (modH^{m-1}), $p = 1, 2, \ldots, q$.*

Proof. In $\overline{H_{ij}^n} \otimes \overline{H_{j'k}^m}$ the given condition implies that $\sum_{p=1}^q \overline{u_p} \otimes \overline{v_p} = 0$. Since $\{\overline{u_p}\}$ is an independent subset it follows that each $\overline{v_p} = \bar{0}$, i.e., $v_p \equiv 0$.

The following lemma shows there is unique factorization modulo appropriate subspaces.

Lemma 1.4.9 *Suppose $ab \equiv cd \ (modH^{n+m-1})$, $m = |a| = |d|$, $n = |b| = |c|$, $m \geq n$, a (i,j)-pure, b (j',k)-pure, c (i,l)-pure, d (l',k)-pure. Then $a \equiv ce \ (modH^{m-1})$, where e is (l',j)-pure of height $m-n$ (or $e = \lambda \in K$ if $m = n$).*

Proof. By Remark 1.4.7 $a \equiv ce + \sum c_p e_p \ (modH^{m-1})$, c, c_p independent $(modH^{n-1})$, $e, e_p \in H^{m-n}_{l'j}$. Thus $ab \equiv ceb + \sum c_p e_p b \equiv cd \ (modH^{m+n-1})$, i.e.,

$$c(eb - d) + \sum c_p(e_p b) \equiv 0 \ (modH^{m+n-1}).$$

By Remark 1.4.8 $eb \equiv d \ (modH_{l'k})$ (hence e is (l',j)-pure of height $m-n$) and $e_p b \equiv 0 \ (modH_{l'k})$. By Remark 1.4.8 again, we conclude that $e_p \equiv 0 \ (modH^{m-n-1})$. Thus $a \equiv ce \ (modH^{m-1})$ and the proof is complete.

The height of an element has the expected properties in view of

Lemma 1.4.10 *$|ab| \leq |a|+|b|$, with strict inequality if and only if for some i,j,k a is (i,j)-pure and b is (j,k)-pure.*

Proof. Let $n = |a|$ and $m = |b|$. Without loss of generality we may assume $n, m \geq 1$. The inequality $|ab| \leq |a| + |b|$ is obvious. Suppose $|ab| < |a| + |b|$. We write $a = a_{ij} + a_{i'j'} \in H^n$, $b = b_{kl} + b_{k'l'} \in H^m$. If $a_{ij} \not\equiv 0 \ (modH^{n-1})$ and $b_{kl} \not\equiv 0 \ (modH^{m-1})$ then by Remark 1.4.8 $a_{ij}b_{kl} \not\equiv 0 \ (modH^{m+n-1})$ unless $j = k$. The conclusion follows from this observation.

Corollary 1.4.11 *If each $dim_K(A_i) > 1$ then $A = A_1 \coprod_K A_2$ is a prime ring.*

Proof. Let $a, b \neq 0$, i.e., $|a| \geq 0$ and $|b| \geq 0$. According to Lemma 1.4.10 we may assume that for some i,j,k a is (i,j)-pure and b is (j,k)-pure. Choosing r to be (j',j')-pure, we see that $arb \neq 0$.

In Corollary 1.4.11, if at least one of the $dim_K(A_i) > 2$, then Lichtman [189] has shown that A is in fact primitive. If each $dim_K(A_i) = 2$ it has been pointed out by Bergman [49] that A is not primitive. We close this section with the following useful remark whose proof is just a formal usage of the universal properties of coproducts and tensor products and we leave the straightforward details for the reader.

Remark 1.4.12 *Let A and B be algebras over a field K and F a field extension of K. Then F-algebras $(A \coprod_K B) \otimes_K F$ and $(A \otimes_K F) \coprod_F (B \otimes_K F)$ are canonically isomorphic.*

1.5 Introduction to First Order Logic

Operations and predicates. Given a set S and a natural number $n > 0$, a mapping $\lambda : \overbrace{S \times S \times \ldots \times S}^{n} \to S$ is called an *n-ary operation* on S and the number n is called the *arity* of the operation λ. A constant mapping $\gamma : S \to S$ is said to be a 0-*ary operation*. In what follows we will identify a 0-ary operation with its image (i.e., γ with $\gamma(S)$). Further, let Z_2 be the two element field. A mapping $\sigma : \overbrace{S \times S \times \ldots \times S}^{n} \to Z_2$ is said to be an *n-ary predicate* on S.

Examples. (1) Let R be a ring. Then 0 is a nullary operation, $-$ is a unary operation and $+, \cdot$ are binary operations. Further, the mapping $\mathcal{P} : R \times R \to Z_2$, given by the rule $\mathcal{P}(r, s) = 1$ if and only if $r = s$, is a predicate. In what follows we will denote $\mathcal{P}(x, y)$ by $\|x = y\|$. Now let $\emptyset \neq T \subseteq R$ be a subset of R. Then the mapping $\mathcal{P}_T : R \to Z_2$ defined by $\mathcal{P}_T(r) = 1$ if and only if $r \in T$, is a predicate also. We will denote it by $\|x \in T\|$.

(2) Let Z_2 be the two element field. Define three binary operations $\wedge$, $\vee$ and $\Rightarrow$ and a unary operation $\neg$ on Z_2 as follows

$$x \vee y = x + y + xy, \; x \wedge y = xy, \; x \Rightarrow y = 1 + x + xy, \; \neg x = 1 + x$$

for all $x, y \in Z_2$. Note that

$$\begin{array}{rcll} x \vee y & = & 1 & \text{if and only if either} \quad x = 1 \quad \textbf{or} \quad y = 1, \\ x \wedge y & = & 1 & \text{if and only if} \quad x = 1 \quad \textbf{and} \quad y = 1, \\ x \Rightarrow y & = & 1 & \text{if and only if } \textbf{either} \quad x = 0 \quad \textbf{or} \quad y = 1, \\ \neg x & = & 1 & \text{if and only if} \quad x = 0. \end{array}$$

Obviously $x \Rightarrow y = \neg x \vee y$ for all $x, y \in Z_2$.

Ω-rings. Let α be an ordinal number. We set

$$W(\alpha) = \{\gamma \mid \gamma \quad \text{is ordinal and} \quad \gamma < \alpha\}.$$

Given a pair $\Omega = (\tau; \alpha)$ (where $\tau : W(\alpha) \to \mathcal{N}$ and $\mathcal{N}$ is the set of all natural numbers), *an Ω-ring R* is a ring R with a set $\Omega_F = \{F_\gamma \mid \gamma \in W(\alpha)\}$ of operations such that the arity of F_γ is equals to $\tau(\gamma)$ for all $\gamma \in W(\alpha)$. It is assumed that $\{0, -, +, \cdot\} \subseteq \Omega_F$.

Example. A ring R together with the set of all its derivations, automorphisms and antiautomorphism is for us the most important example of an Ω-ring.

Given two Ω-rings R and S, the mapping $f : R \to S$ is said to be *a homomorphism of Ω-rings* if $F_\gamma(r_1, \ldots, r_{\tau(\gamma)})^f = F_\gamma(r_1^f, \ldots, r_{\tau(\gamma)}^f)$ for all $r_1, \ldots, r_{\tau(\gamma)} \in R$ and $\gamma \in W(\alpha)$. A subset $I \subseteq R$ of the Ω-ring R is said to be R *an ideal of an Ω-ring* if $F_\gamma(r_1 + i_1, \ldots, r_{\tau(\gamma)} + i_{\tau(\gamma)}) - F_\gamma(r_1, \ldots, r_{\tau(\gamma)}) \in I$ for all $r_1, \ldots, r_{\tau(\gamma)} \in R$, $i_1, \ldots, i_{\tau(\gamma)} \in I$ and $\gamma \in W(\alpha)$. It is easy to see that an ideal of the Ω-ring R is an ideal of the ring R. Clearly the kernel $\ker(f)$ of a homomorphism f of Ω-rings R and S is an ideal of the Ω-ring R. Similarly to that of an ideal and a homomorphism one may easily formulate the notions of a factor Ω-ring, variety of Ω-rings and a free Ω-ring of a given variety generated by a given set X. Being only interested in Ω-rings in the case when the set $\Omega_F = \Omega_d \cup \Omega_e \cup \Omega_a \cup \{0, -, +, \cdot\}$ consists of certain sets (possibly empty) of derivations (Ω_d), endomorphisms (Ω_e) and antiendomorphisms (Ω_a) (such Ω-rings form a variety determined by identities of the type $(xy)^d = x^d y + xy^d$, $d \in \Omega_d$, etc.), we proceed to describe a free Ω-ring in this case.

Let S be the free semigroup (with 1) generated by the set $\Omega_d \cup \Omega_e \cup \Omega_a$ and let $\mathcal{Z}$ be the ring of integers. We set $Y = X \times S$, which we may write suggestively as X^S, and $K = \mathcal{Z}<Y>$. Define a mapping $\sigma : X \to K$, setting $x^\sigma = (x, 1) = x^1 \in Y \subseteq K$. Further, let $\omega \in \Omega_d \cup \Omega_e \cup \Omega_a$. We set $(x^s)^\omega = x^{s\omega}$ for all $x \in X$, $s \in S$. Since ω is either a derivation, endomorphism, or antiendomorphism, there exists a unique extension of the mapping ω up to, respectively, a derivation, endomorphism or antiendomorphism of K. Now one may easily check that $(X; \sigma; K)$ is the free Ω-ring generated by the set X.

Terms. Let $X = \{x_1, x_2, \ldots, x_n, \ldots\}$ be an infinite set and $\mathcal{T}_\Omega$ the free Ω-ring generated by X. Then any element $t \in \mathcal{T}_\Omega$ is called *a term of the signature* Ω. Given any $\gamma \in W(\alpha)$ and $y_1, y_2, \ldots, y_{\tau(\gamma)} \in X$ (not necessarily distinct), we choose any linear ordering $\{z_1, z_2, \ldots, z_m\}$ of the set $\{y_1, y_2, \ldots, y_{\tau(\gamma)}\}$ where $z_i \neq z_j$ for all $1 \leq i \neq j \leq m$ and we will use the notation $t = t(z_1, z_2, \ldots, z_m)$ for the term $t = F_\gamma(y_1, y_2, \ldots, y_{\tau(\gamma)})$. We let

$$\mathcal{X}(t) = \{y_1, y_2, \ldots, y_{\tau(\gamma)}\} = \{z_1, z_2, \ldots, z_m\}$$

be the set of all variables involved in t. Let now $\theta \in W(\alpha)$, $n = \tau(\theta)$ and let $t_i = t_i(y_{i,1}, \ldots, y_{i,m_i})$, $i = 1, 2, \ldots, n$, be terms. Choosing any linear ordering $\{x_1, x_2, \ldots, x_m\}$ of the set $\cup_{i=1}^n \mathcal{X}(t_i)$, we will use the notations

$$\begin{aligned} t &= t(x_1, x_2, \ldots, x_m) = F_\theta(t_1, t_2, \ldots, t_n), \\ & \mathcal{X}(t) = \bigcup_{i=1}^n \mathcal{X}(t_i). \end{aligned}$$

Substitutions. Given any Ω-ring R and a mapping $\eta : X \to R$, there exists a unique extension of η to a homomorphism of Ω-rings $\mathcal{T}_\Omega \to R$. Therefore we may identify the set of all homomorphisms of Ω-rings $\mathcal{T}_\Omega \to R$ with the set $Map(X; R)$ of all mappings of the set X into R. Let $t = t(x_1, x_2, \ldots, x_n) \in \mathcal{T}_\Omega$ and $\eta \in Map(X; R)$. We set

$$t(x_1^\eta, x_2^\eta, \ldots, x_n^\eta) = t^\eta.$$

Elements of the set $Map(X; R)$ are called *substitutions*.

Given any $u \in X$ and $v \in R$ define the mapping $\rho_{u,v} : Map(X; R) \to Map(X; R)$, setting

$$u^{\rho_{u,v}(\eta)} = v \quad \text{and} \quad x^{\rho_{u,v}(\eta)} = x^\eta \quad \text{for all} \quad x \in X,\ x \neq u.$$

Let $U = (x_1, x_2, \ldots, x_n) \in X^{(n)}$ and $V = (v_1, v_2, \ldots, v_n) \in R^{(n)}$ where $X^{(n)}$ and $R^{(n)}$ are n-th Cartesian power of X and R respectively. Assuming that $x_i \neq x_j$ for all $i \neq j$, we set

$$\rho_{U,V} = \rho_{x_1,v_1} \rho_{x_2,v_2} \cdots \rho_{x_n,v_n}.$$

Consider now a term t such that $t = t(x_1, x_2, \ldots, x_n)$. Obviously $t^{\rho_{U,V}(\eta)} = t(v_1, v_2, \ldots, v_n)$ for all $\eta \in Map(X; R)$.

Now we introduce the following useful notations. For any $y, x_1, x_2, \ldots, x_{m+1} \in X$ and $1 \leq i \leq m$, we set

$$(x_1, x_2, \ldots, x_{m+1})^{[i]} = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{m+1});$$
$$(x_1, x_2, \ldots, x_m)^{[i;y]} = (x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_m).$$

Ω-Δ-rings. Given pairs $\Omega = (\tau; \alpha)$ and $\Delta = (\sigma; \beta)$ (where $\tau : W(\alpha) \to \mathcal{N}$ and $\sigma : W(\beta) \to \mathcal{N}$), an *$\Omega$-$\Delta$-ring* R is an Ω-ring R with a set $\Delta_P = \{P_\gamma \mid \gamma \in W(\beta)\}$ of predicates such that the arity of P_γ is equal to $\sigma(\gamma)$ for all $\gamma \in W(\beta)$.

Let now $\{R_t \mid t \in T\}$, be a family of Ω-Δ-rings. We proceed to describe the *Cartesian product* $H = \prod_{t \in T} R_t$ of Ω-Δ-rings. We consider H as the set of all mappings $h : T \to \bigcup_{t \in T} R_t$ such that $h(t) \in R_t$ for all $t \in T$. Defining operations pointwise, we obtain an Ω-ring structure on H. Given any $\gamma \in W(\beta)$ and $h_1, h_2, \ldots, h_{\sigma(\gamma)} \in H$, we set $P_\gamma(h_1, h_2, \ldots, h_{\sigma(\gamma)}) = 1$ if and only if $P_\gamma(h_1(t), h_2(t), \ldots, h_{\sigma(\gamma)}(t)) = 1$ for all $t \in T$.

Note, that the "behavior" of predicates under taking of Cartesian products of Ω-Δ-rings "coincides" with the behavior of that predicate which is most important for us, namely, $||x = y||$.

First order formulas. Consider the set $\mathcal{L}$ of *logical* symbols

$\wedge$ (for conjunction, read **AND**),
$\vee$ (for disjunction, read **OR**),
$\neg$ (for negation, read **NOT**),
$\Rightarrow$ (for implication, read **IMPLIES**),
$\forall$ (for universal quantification, read **FOR EVERY**),
$\exists$ (for existential quantification, read **THERE EXISTS**),
$=$ (for equality, read **EQUALS**).

Letting $\mathcal{P}_\Delta$ denote the set of all formal predicate symbols

$$\{P_\gamma(t_1, t_2, \ldots, t_{\sigma(\gamma)}) \mid \gamma < \beta,\ t_1, t_2, \ldots, t_{\sigma(\gamma)} \in \mathcal{T}_\Omega\}$$

we define $\mathcal{S}$ to be the free semigroup generated by the disjoint sets $\mathcal{L}$, $\mathcal{T}_\Omega$, $\mathcal{P}_\Delta$ and $\{\{,\ \},\ (,\ ),\ [,\ ],\ ||\}$. Now we proceed to define the first order formulas (which we shall simply refer to as *formulas*) as a subset $\mathcal{F}_{\Omega,\Delta}$ of $\mathcal{S}$. Formulas ϕ, together with associated sets of *free variables* $\mathcal{X}(\phi)$ and *complexity* $Compl(\phi)$, are defined inductively.

(i) If t_1 and t_2 are terms, then the element $||t_1 = t_2|| \in \mathcal{S}$ is called a formula. Choosing any linear ordering $\{z_1, z_2, \ldots, z_m\}$ of the set $\mathcal{X}(t_1) \cup \mathcal{X}(t_2)$, we set

$$\begin{aligned} &\phi = \phi(z_1, \ldots, z_m) = ||t_1 = t_2||, \\ &\mathcal{X}(\phi) = \mathcal{X}(t_1) \cup \mathcal{X}(t_2) \quad \text{and} \quad Compl(\phi) = 1. \end{aligned}$$

Such formulas are called *atomic.*

(ii) For any predicate symbol $P_\gamma \in \Delta$ and any terms $t_1, \ldots, t_n$ where $n = \sigma(\gamma)$ the element $P_\gamma(t_1, t_2, \ldots, t_n) \in \mathcal{P}_\Delta$ is said to be a formula and, choosing an arbitrary linear ordering $\{z_1, \ldots, z_m\}$ of the set $\bigcup_{i=1}^n \mathcal{X}(t_i)$, we set

$$\begin{aligned} &\psi = \psi(z_1, \ldots, z_m) = P_\gamma(t_1, t_2, \ldots, t_n), \\ &\mathcal{X}(\psi) = \bigcup_i \mathcal{X}(t_i) \quad \text{and} \quad Compl(\psi) = 1. \end{aligned}$$

Such formulas are also called *atomic*.

(iii) If ϕ is a formula, then $\neg\phi$ is a formula and we set

$$\mathcal{X}(\neg\phi) = \mathcal{X}(\phi) \quad \text{and} \quad Compl(\neg\phi) = Compl(\phi) + 1.$$

(iv) If ϕ and ψ are formulas, then $\phi \vee \psi$, $\phi \wedge \psi$ and $\phi \Rightarrow \psi$ are formulas and we set

$$\begin{aligned} \mathcal{X}(\phi \vee \psi) &= \mathcal{X}(\phi \wedge \psi) = \mathcal{X}(\phi \Rightarrow \psi) = \mathcal{X}(\phi) \cup \mathcal{X}(\psi) \quad \text{and} \\ Compl(\phi \vee \psi) &= Compl(\phi \wedge \psi) = Compl(\phi \Rightarrow \psi) \\ &= max\{Compl(\phi),\ Compl(\psi)\} + 1. \end{aligned}$$

(v) If ϕ is a formula and $x \in X$, then $(\forall x)\phi$ and $(\exists x)\psi$ are formulas and we set

$$\begin{aligned} \mathcal{X}\left((\forall x)\phi\right) &= \mathcal{X}\left((\exists x)\phi\right) = \mathcal{X}(\phi) \setminus \{x\} \quad \text{and} \\ Compl\left((\forall x)\phi\right) &= Compl\left((\exists x)\phi\right) = Compl(\phi) + 1. \end{aligned}$$

If ϕ is a formula and $\mathcal{X}(\phi) = \emptyset$, then the formula ϕ is called *a sentence* .

The notation in general $\phi = \phi(y_1, y_2, \ldots, y_n)$ is introduced analogously to that for the cases **(i)** and **(ii)**. We only note, that if either $\psi = (\forall y_i)\phi$ or $\psi = (\exists y_i)\phi$, then $\psi = \psi(y_1, \ldots, y_n)^{[i]}$.

Notations. We shall write $\|x \notin T\|$ instead of $\neg\|x \in T\|$ and $\|x \neq y\|$ instead of $\neg\|x = y\|$.

Formulas and substitutions. We shall put into correspondence with any substitution $\eta \in Map(X; R)$ of an Ω-Δ-ring R the mapping $\bar{\eta} : \mathcal{F}_{\Omega,\Delta} \to Z_2$. We proceed by induction on the complexity of formulas.

If $\phi = \|t_1 = t_2\|$, then $\phi^{\bar{\eta}} = 1$ if and only if $t_1^{\eta} = t_2^{\eta}$. Consider now the case $\phi = P_{\gamma}(t_1, t_2, \ldots, t_{\sigma(\gamma)})$. Then we set $\phi^{\bar{\eta}} = P_{\gamma}(t_1^{\eta}, t_2^{\eta}, \ldots, t_{\sigma(\gamma)}^{\eta})$.

Suppose that our mapping $\bar{\eta}$ is defined on formulas of complexity $\leq m$ and $Compl(\phi), Compl(\psi) \leq m$. We set

$$(\neg\phi)^{\bar{\eta}} = \neg\phi^{\bar{\eta}},$$

$$\begin{aligned}(\phi \vee \psi)^{\bar{\eta}} &= \phi^{\bar{\eta}} \vee \psi^{\bar{\eta}},\\ (\phi \wedge \psi)^{\bar{\eta}} &= \phi^{\bar{\eta}} \wedge \psi^{\bar{\eta}},\\ (\phi \Rightarrow \psi)^{\bar{\eta}} &= \phi^{\bar{\eta}} \Rightarrow \psi^{\bar{\eta}}.\end{aligned}$$

Further, $((\forall x)\phi)^{\bar{\eta}} = 1$ if and only if $\phi^{\overline{\rho_{x,r}(\eta)}} = 1$ for all $r \in R$. Analogously, $((\exists x)\phi)^{\bar{\eta}} = 1$ if and only if $\phi^{\overline{\rho_{x,r}(\eta)}} = 1$ for some $r \in R$.

Proposition 1.5.1 *Let $\phi = \phi(y_1, y_2, \ldots, y_n)$ be a formula. Consider the subsets $Y = (y_1, \ldots, y_n) \in X^{(n)}$ and $V = (v_1, \ldots, v_n) \in R^{(n)}$. Then $\phi^{\overline{\rho_{Y,V}(\eta)}} = \phi^{\overline{\rho_{Y,V}(\theta)}}$ for all $\eta, \theta \in Map(X; R)$.*

Proof. We proceed by induction on the complexity of ϕ. Assume that $Compl(\phi) = 1$. Consider the case

$$\phi = \|t_1(y_{i_1}, \ldots, y_{i_m}) = t_2(y_{j_1}, \ldots, y_{j_t})\|,$$

where $\mathcal{X}(t_1) \cup \mathcal{X}(t_2) = Y$. Then

$$\phi^{\overline{\rho_{Y,V}(\eta)}} = \|t_1(v_{i_1}, \ldots, v_{v_m}) = t_2(v_{j_1}, \ldots, v_{j_t})\| = \phi^{\overline{\rho_{Y,V}(\theta)}}.$$

The case $\phi = P_\gamma(t_1, \ldots, t_n)$ is considered analogously.

Suppose now that $Compl(\phi) = m + 1$ and our statement is proved for formulas of complexity less than or equal to m. Consider the case $\phi = \neg\psi(y_1, \ldots, y_n)$. Then we have

$$\begin{aligned}\phi^{\overline{\rho_{Y,V}(\eta)}} &= \neg\psi^{\overline{\rho_{Y,V}(\eta)}} = \neg\psi^{\overline{\rho_{Y,V}(\theta)}}\\ &= \phi^{\overline{\rho_{Y,V}(\theta)}}.\end{aligned}$$

The cases $\phi = \psi_1 \vee \psi_2$, $\phi = \psi_1 \wedge \psi_2$ and $\phi = \psi_1 \Rightarrow \psi_2$ are considered similarly. Assume now that $\phi = (\forall z)\psi(z_1, \ldots, z_m)$ where $(z_1, z_2, \ldots, z_m)^{[i]} = (y_1, y_2, \ldots, y_n)$ (for simplicity we assume that $z = z_i$ for some $1 \leq i \leq m$). Now we have

$$\phi^{\overline{\rho_{Y,V}(\eta)}} = 1 \quad \text{if and only if} \quad \psi^{\overline{\rho_{z,v}\rho_{Y,V}(\eta)}} = 1 \quad \text{for all} \quad v \in R.$$

Since $\rho_{z,r}\rho_{Y,V} = \rho_{Y',V'}$ where $Y' = (z, y_1, \dots, y_n)$ and $V = (v, v_1, \dots, v_n)$, by the inductive assumption we have

$$\psi^{\overline{\rho_{z,v}\rho_{Y,V}(\eta)}} = \psi^{\overline{\rho_{z,v}\rho_{Y,V}(\theta)}}.$$

Therefore $\phi^{\overline{\rho_{Y,V}(\eta)}} = \phi^{\overline{\rho_{Y,V}(\theta)}}$. The last case $\phi = (\exists z)\psi$ is considered analogously.

Let $\phi = \phi(y_1, y_2, \dots, y_n)$ be a formula, $\eta \in Map(X; R)$. For any subset $v_1, v_2, \dots, v_n \in R$ we set $Y = \{y_1, y_2, \dots, y_n\}$, $V = \{v_1, v_2, \dots, v_n\}$ and

$$\phi(v_1, v_2, \dots, v_n) = \phi^{\overline{\rho_{Y,V}(\eta)}}.$$

It follows from Proposition 1.5.1, that $\phi(v_1, v_2, \dots, v_n) \in Z_2$ is independent of η. We will write

$$R \models \phi(v_1, v_2, \dots, v_n)$$

if $\phi(v_1, v_2, \dots, v_n) = 1$. In this case we will say that the formula $\phi(v_1, v_2, \dots, v_n)$ is *true* in the Ω-Δ-ring R. Otherwise we will say that the formula $\phi(v_1, v_2, \dots, v_n)$ is *false* .

Examples. Let R be a ring.

(1) Consider the formula $\phi_1 = (\forall x)(\forall y)\|xy = yx\|$. Then $R \models \phi_1$ if and only if R is commutative.

(2) Let $\phi_2(x) = (\forall y)\|xy = yx\|$. Given any $r \in R$, $R \models \psi_2(r)$ if and only if r is a central element of R.

(3) Now let $\phi_3(x) = (\forall y)(\exists z)\,[\|y \neq 0\| \Rightarrow \{\,\|yz \neq 0\| \wedge \|xyz = 0\|\,\}]$. For an element $r \in R$, $R \models \phi_3(r)$ if and only if the right annihilator of r in R is an essential right ideal of R.

Two formulas $\phi = \phi(y_1, y_2, \dots, y_n)$ and $\psi = \psi(z_1, z_2, \dots, z_m)$ are said to be *equivalent*, if for any Ω-Δ-ring R and any substitution $\eta \in Map(X, R)$, the formula $\phi(x_1^\eta, \dots, x_n^\eta)$ is true in R if and only if $\psi(z_1^\eta, \dots, z_m^\eta)$ is true.

The following proposition is easily proved by induction on complexity of formulas.

Proposition 1.5.2 *Let $\phi = \phi(x_1, x_2, \ldots, x_n)$, ψ be formulas and $z \in X \setminus \mathcal{X}(\phi) \setminus \mathcal{X}(\psi)$. Then the following formulas are equivalent:*

$$\begin{array}{rcl}
\phi & \textit{and} & \neg(\neg\phi), \\
\neg(\phi \wedge \psi) & \textit{and} & (\neg\phi) \vee (\neg\psi), \\
\neg(\phi \vee \psi) & \textit{and} & (\neg\phi) \wedge (\neg\psi), \\
\phi \Rightarrow \psi & \textit{and} & (\neg\phi) \vee \psi, \\
\neg\left((\forall x)(\neg\phi)\right) & \textit{and} & (\exists x)(\phi), \\
\neg\left((\exists x)(\neg\phi)\right) & \textit{and} & (\forall x)(\phi), \\
\phi \wedge ((\forall x_i)\psi) & \textit{and} & (\forall x_i)\left(\phi(x_1, x_2, \ldots, x_n)^{[i;z]} \wedge \psi\right), \\
\phi \wedge ((\exists x_i)\psi) & \textit{and} & (\exists x_i)\left(\phi(x_1, x_2, \ldots, x_n)^{[i;z]} \wedge \psi\right), \\
\phi \vee ((\forall x_i)\psi) & \textit{and} & (\forall x_i)\left(\phi(x_1, x_2, \ldots, x_n)^{[i;z]} \vee \psi\right), \\
\phi \vee ((\exists x_i)\psi) & \textit{and} & (\exists x_i)\left(\phi(x_1, x_2, \ldots, x_n)^{[i;z]} \vee \psi\right), \\
\phi & \textit{and} & (\forall z)\phi, \\
\phi & \textit{and} & (\exists z)\phi.
\end{array}$$

The next two corollaries follow immediately by an induction on the complexity of formulas from Proposition 1.5.2.

Corollary 1.5.3 *Any formula ϕ is equivalent to a formula of the form $(Q_1 y_1)(Q_2 y_2) \ldots (Q_m y_m)\psi$, where $Q_i \in \{\forall, \exists\}$, $i = 1, 2, \ldots, m$, and the formula ψ does not contain quantifiers $\forall$ and $\exists$.*

Corollary 1.5.4 *Any formula is equivalent to a formula containing only atomic formulas, symbols $\neg$, $\wedge$, $\exists$, variables and bracket symbols.*

Let $\phi = \phi(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$ be a formula such that

$$\{x_{i_1}, x_{i_2}, \ldots, x_{i_n}\} \subseteq \{x_1, x_2, \ldots, x_n\}.$$

Define a new formula ψ in free variables $x_1, x_2, \ldots, x_n$ as follows $\psi(x_1, x_2, \ldots, x_n) = \phi(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$. Then clearly

$$\text{The formulas } \phi \text{ and } \psi \text{ are equivalent.} \tag{1.7}$$

Horn formulas and multiplicative stability. The reader has seen already that formulas provide us with a formal way of writing properties of Ω-Δ-rings and their elements. It is rather interesting to note that the stability of properties under taking of Cartesian products mainly depends on the structure of the corresponding formulas. Now we shall describe an important class of formulas, stable under taking Cartesian products.

A formula ϕ is said to be a *Horn* formula if it is equivalent to a formula of the type $(Q_1y_1)(Q_2y_2)\ldots(Q_my_m)\psi$, where $Q_i \in \{\forall, \exists\}$, $i = 1, 2, \ldots, m$, the formula ψ does not contain quantifiers $\forall$ and $\exists$ and is the conjunction of formulas each of which is either **(a)** an atomic formula; **(b)** the disjunction of one atomic formula and several negations of atomic formulas; or **(c)** the disjunction of negations of atomic formulas.

A formula $\phi = \phi(y_1, y_2, \ldots, y_n)$ is called *multiplicatively stable* , if the following holds: for any family $\{R_i \mid i \in I\}$ of Ω-Δ-rings and all $h_1, h_2, \ldots, h_n \in H = \prod_{i \in I} R_i$ the relations

$$R_i \models \phi(h_1(i), h_2(i), \ldots, h_n(i)), \quad \text{for all} \quad i \in I,$$

imply that

$$H \models \phi(h_1, h_2, \ldots, h_n).$$

Further a multiplicatively stable formula $\phi = \phi(y_1, y_2, \ldots, y_n)$ is said to be a *strictly multiplicatively stable formula*, if for all $h_1, h_2, \ldots, h_n \in H$ the relation $H \models \phi(h_1, h_2, \ldots, h_n)$ implies that $R_i \models \phi(h_1(i), \ldots, h_n(i))$ for all $i \in I$.

Example. The formula

$$\phi = (\forall x)(\forall y)\,[(x = 0) \vee (y = 0) \vee (xy \neq 0)]$$

is not multiplicatively stable, since the Cartesian product of domains is no longer a domain. But the formula

$$\psi = (\forall x)\left[(x = 0) \vee (x^2 \neq 0)\right]$$

is multiplicatively stable.

Theorem 1.5.5 (A. Horn [196]) *Every Horn formula is multiplicatively stable.*

Proof. It immediately follows from the definitions that atomic formulas are strictly multiplicatively stable.

Consider now the case

$$\phi = \vee_{j=1}^{n}(\neg\psi_j),$$

where ψ_j, $j = 1, 2, \ldots, n$, are atomic formulas. By (1.7) we may assume that $\mathcal{X}(\psi_i) = \mathcal{X}(\psi_j)$ for all i, j. Let

$$\phi = \phi(y_1, \ldots, y_m),\ \psi_j = \psi_j(y_1, \ldots, y_m),\ 1 \leq j \leq n$$

and $h_1, h_2, \ldots, h_m \in H$. Suppose that $R_i \models \phi(h_1(i), \ldots, h_m(i))$ for all $i \in I$. Fix any $t \in I$. We have $R_t \models \phi(h_1(t), \ldots, h_m(t))$ and so $R_t \models (\neg\psi_j(h_1(t), \ldots, h_m(t)))$ for some $1 \leq j \leq n$. Since all atomic formulas are strictly multiplicatively stable, we see that $H \models (\neg\psi_j(h_1, \ldots, h_m))$. Therefore $H \models \phi(h_1, \ldots, h_m)$. Let now $\phi = \psi_1 \vee \left[\vee_{j=2}^{n}(\neg\psi_j)\right]$. Again we suppose that $R_i \models \phi(h_1(i), \ldots, h_m(i))$ for all $i \in I$. If for some $t \in I$ and $2 \leq j \leq n$ we have that $R_t \models (\neg\psi_j(h_1(t), \ldots, h_m(t)))$, then as above one may show that $H \models \phi(h_1, \ldots, h_m)$. Therefore without loss of generality we may assume that formulas $\neg\psi_j(h_1(i), \ldots, h_m(i))$ are false in R_i for all $j = 2, 3, \ldots, n$ and $i \in I$. Since $R_i \models \phi(h_1(i), \ldots, h_m(i))$ for all $i \in I$, $R_i \models \psi_1(h_1(i), \ldots, h_m(i))$ for all $i \in I$ also. Then $H \models \psi_1(h_1, \ldots, h_m)$ and $H \models \phi(h_1, \ldots, h_m)$.

If ψ_j, $j = 1, 2, \ldots, n$, are multiplicatively stable formulas, then one may easily check that the formula $\phi = \wedge_{j=1}^{n}\psi_j$ is multiplicatively stable also.

Let $1 \leq j \leq n$ and $\phi(y_1, \ldots, y_m)^{[j]} = (\exists y_j)\psi(y_1, \ldots, y_m)$ where ψ is a multiplicatively stable formula. Suppose that

$$R_i \models \phi(h_1(i), \ldots, h_{j-1}(i), h_{j+1}(i), \ldots, h_m(i))$$

for all $i \in I$, where $h_1, \ldots, h_{j-1}, h_{j+1}, \ldots, h_n \in H$. Then for every $i \in I$ there exists an element $h_j(i) \in R_i$ such that $R_i \models \psi(h_1(i), \ldots, h_m(i))$. Since ψ is multiplicatively stable, $H \models \psi(h_1, \ldots, h_m)$. But then again

$$H \models \phi(h_1, \ldots, h_{j-1}, h_{j+1}, \ldots, h_m).$$

The case when $\phi = (\forall y)\psi$ is considered analogously. Thus the theorem is proved.

Ultrafilters. Let I be an infinite set and $Exp(I)$ the set of all subsets of I. A subset $\mathcal{T} \subseteq Exp(I)$ is said to be a *filter* on the set I, if it does not contain the empty subset and for every natural number n and all $T_1, T_2, \ldots, T_n \in \mathcal{T}$, $\bigcap_{j=1}^{n} T_j \in \mathcal{T}$.

Examples (1) Given any $i_0 \in I$, we set $\mathcal{T}(i_0) = \{T \subseteq I \mid i_0 \in T\}$. Clearly $\mathcal{T}(i_0)$ is a filter.

(2) We set $\mathcal{T}_\infty = \{T \subseteq I \mid |I \setminus T| < \infty\}$. Obviously $\mathcal{T}_\infty$ is a filter.

We note that the set of all filters on I is partially ordered by inclusion. A filter $\mathcal{T}$ on the set I is said to be an *ultrafilter* on I if it is a maximal element in the partially ordered set of all filters on I.

Example. Clearly the filter $\mathcal{T}(i_0)$ is an ultrafilter on I. Such ultrafilters are called *principal*.

Proposition 1.5.6 *Let I be an infinite set, $\mathcal{T}$ an ultrafilter on I and $X \subseteq I$. Then:*

(a) Any filter on I is contained in some ultrafilter;

(b) $I \in \mathcal{T}$;

(c) if $X \cap T \neq \emptyset$ for all $T \in \mathcal{T}$, then $X \in \mathcal{T}$;

(d) *if $T \in \mathcal{T}$ and $T = \bigcup_{j=1}^{n} B_j$, then $B_j \in \mathcal{T}$ for some $1 \leq j \leq n$;*

(e) *a filter $\mathcal{F}$ on I is an ultrafilter if and only if for any $A \subseteq I$ either $A \in \mathcal{F}$, or $I \setminus A \in \mathcal{F}$;*

(f) *if $T \in \mathcal{T}$ and $T \subseteq A \subseteq I$, then $A \in \mathcal{T}$.*

Proof. The first statement follows easily from Zorn's lemma. The second one is obvious.

(c) Consider the collection $\mathcal{T}' = \mathcal{T} \cup \{X \cap T \mid T \in \mathcal{T}\}$ of subsets of I. Clearly it is a filter and $\mathcal{T} \subseteq \mathcal{T}'$. Since $\mathcal{T}$ is a maximal element of the set of all filters on I, $\mathcal{T} = \mathcal{T}'$. So $X \in \mathcal{T}$.

(d) Suppose the contrary. By **(c)** for every $1 \leq j \leq n$ there exist an element $A_j \in \mathcal{T}$ such that $B_j \cap A_j = \emptyset$. Letting A denote the intersection of all A_j, we infer that $A \cap B_j = \emptyset$. Therefore $A \cap T = \emptyset$, a contradiction to $A, T \in \mathcal{T}$. Hence $B_j \in \mathcal{T}$ for some j.

(e) Taking into account the already proved statement **(c)**, we have only to prove that if a filter $\mathcal{F}$ on I is such that for any $A \subseteq I$ either $A \in \mathcal{F}$, or $I \setminus A \in \mathcal{F}$, then $\mathcal{F}$ is an ultrafilter. Again suppose the contrary. Let $\mathcal{F} \subset \mathcal{H}$ for some filter $\mathcal{H}$. Then there exists an element $A \in \mathcal{H}$ which does not belong to $\mathcal{F}$. By assumption we then have that $I \setminus A \in \mathcal{F} \subset \mathcal{H}$. But $A \cap (I \setminus A) = \emptyset$, which contradicts the definition of a filter. Thus $\mathcal{F}$ is an ultrafilter. The last statement follows from **(c)**.

Corollary 1.5.7 *Let I be an infinite set and $\mathcal{T}$ an ultrafilter on I. Then either $\mathcal{T}$ is a principal ultrafilter, or $\mathcal{T}_\infty \subseteq \mathcal{T}$.*

Proof. Obviously an ultrafilter $\mathcal{T}$ is principal if and only if there exists an element $i_0 \in I$ such that $\{i_0\} \in \mathcal{T}$. Assume that $\mathcal{T}$ is not principal. Let $J \subseteq I$ be any finite subset of I. Since $\{j\} \notin \mathcal{T}$ for all $j \in J$, it follows from Proposition 1.5.6, that $J \notin \mathcal{T}$. Then again by Proposition 1.5.6 we have that $I \setminus J \in \mathcal{T}$. Thus $\mathcal{T}_\infty \subseteq \mathcal{T}$.

Ultraproducts. Given any family $\{R_i \mid i \in I\}$, of Ω-Δ-rings, where I is an infinite set, and an element $h \in H = \prod_{i \in I} R_i$, we set

$$I(h) = \{i \in I \mid h(i) = 0\}.$$

For an ultrafilter $\mathcal{T}$ on I, we set

$$I(\mathcal{T}) = \{h \in \prod_{i \in I} R_i \mid I(h) \in \mathcal{T}\}.$$

We claim that $I(\mathcal{T})$ is an ideal of the Ω-ring $H = \prod_{i \in I} R_i$. Indeed, for all $h, g \in H$ we have $I(-h) = I(h)$, $I(hg) \supseteq I(h) \cap I(g)$, $I(h+g) \supseteq I(h) \cap I(g)$. It is now immediate that $I(\mathcal{T})$ is an ideal of the ring H. Let $\gamma \in W(\alpha)$, $n = \tau(\gamma)$, $g_1, g_2, \ldots, g_n \in H$, $h_1, h_2, \ldots, h_n \in I(\mathcal{T})$ and $h = F_\gamma(g_1 + h_1, g_2 + h_2, \ldots, g_n + h_n) - F_\gamma(g_1, g_2, \ldots, g_n)$. Since $I(h) \supseteq \bigcap_{t=1}^{n} I(h_t) \in \mathcal{T}$, $h \in I(\mathcal{T})$. Thus $I(\mathcal{T})$ is an ideal of the Ω-ring H. Consider the factor Ω-ring $H/I(\mathcal{T})$. Now we proceed to describe an Ω-Δ-ring structure on it. Given any $\gamma \in W(\beta)$, $h_1, h_2, \ldots, h_{\sigma(\gamma)} \in H$, we set

$$P_\gamma(h_1 + I(\mathcal{T}), h_2 + I(\mathcal{T}), \ldots, h_{\sigma(\gamma)} + I(\mathcal{T})) = 1$$

if and only if

$$\{i \in I \mid P_\gamma(h_1(i), h_2(i), \ldots, h_{\sigma(\gamma)}(i)) = 1\} \in \mathcal{T}.$$

The factor Ω-Δ-ring $H/I(\mathcal{T})$ is called the *ultraproduct* of Ω-Δ-rings R_i, $i \in I$, and is denoted by $\prod_{i \in I} R_i/\mathcal{T}$. The canonical image of an element $h \in H$ in $H/I(\mathcal{T})$ is denoted by $h\mathcal{T}$.

Theorem 1.5.8 (Los [196]) *Let $\{R_i \mid i \in I\}$ be an infinite family of Ω-Δ-rings, $H = \prod_{i \in I} R_i$, $\phi(y_1, y_2, \ldots, y_n)$ a first order formula in free variables $y_1, y_2, \ldots, y_n$, $h_1, h_2, \ldots, h_n \in H$ and $\mathcal{T}$ an ultrafilter on I. Then*

$$\prod_{i \in I} R_i/\mathcal{T} \models \phi(h_1\mathcal{T}, h_2\mathcal{T}, \ldots, h_n\mathcal{T})$$

if and only if

$$I_\phi(h_1, \ldots, h_n) = \{i \in I \mid R_i \models \phi(h_1(i), \ldots, h_n(i))\} \in \mathcal{T}.$$

Proof. Suppose that $Compl(\phi) = 1$. Consider the case when

$$\phi(y_1, y_2, \dots, y_n) = \|t_1(y_{i_1}, \dots, y_{i_m}) = t_2(y_{j_1}, \dots, y_{j_t})\|,$$

where $\{y_1, y_2, \dots, y_n\} = \mathcal{X}(t_1) \cup \mathcal{X}(t_2)$. Clearly

$$\prod_{i \in I} R_i/\mathcal{T} \models \phi(h_1\mathcal{T}, \dots, h_n\mathcal{T})$$

if and only if

$$t_1(h_{i_1}\mathcal{T}, \dots, t_{i_m}\mathcal{T}) = t_2(h_{j_1}\mathcal{T}, \dots, t_{j_t}\mathcal{T}).$$

The last condition is equivalent to

$$t_1(h_{i_1}\mathcal{T}, \dots, t_{i_m}\mathcal{T}) - t_2(h_{j_1}\mathcal{T}, \dots, t_{j_t}\mathcal{T}) = 0,$$

which in turn is equivalent to

$$\{i \in I \mid t_1(h_{i_1}(i), \dots, h_{i_m}(i)) - t_2(h_{j_1}(i), \dots, t_{j_t}(i) = 0\} \in \mathcal{T}.$$

But

$$\{i \in I \mid t_1(h_{i_1}(i), \dots, h_{i_m}(i)) - t_2(h_{j_1}(i), \dots, t_{j_t}(i) = 0\}$$
$$= I_\phi(h_1, h_2, \dots, h_n).$$

Therefore

$$\prod_{i \in I} R_i/\mathcal{T} \models \phi(h_1\mathcal{T}, \dots, h_n\mathcal{T})$$

if and only if

$$I_\phi(h_1, h_2, \dots, h_n) \in \mathcal{T}.$$

The case $\phi = P_\gamma(t_1, t_2, \dots, t_{\sigma(\gamma)})$ follows directly from the definitions.

Assume now that our statement is proved for the formula $\psi(y_1, \dots, y_n)$ and $\phi = \neg\psi$. It immediately follows from the definition that

$$I_\phi(h_1, h_2, \dots, h_n) = I \setminus I_\psi(h_1, h_2, \dots, h_n).$$

We have

$$\prod_{i\in I} R_i/\mathcal{T} \models \phi(h_1\mathcal{T}, h_2\mathcal{T}, \ldots, h_n\mathcal{T})$$

if and only if $\psi(h_1\mathcal{T}, h_2\mathcal{T}, \ldots, h_n\mathcal{T})$ is false in $\prod_{i\in I} R_i/\mathcal{T}$. By assumption the last is equivalent to $I_\psi(h_1, h_2, \ldots, h_n) \notin \mathcal{T}$, which in turn is equivalent to $I_\phi(h_1, h_2, \ldots, h_n) \in \mathcal{T}$ (see Proposition 1.5.6).

Suppose that $\phi = \psi_1 \wedge \psi_2$ and our statement is proved for formulas ψ_1 and ψ_2. By (1.7) we may assume that

$$\phi = \phi(y_1, y_2, \ldots, y_m),\ \psi_t = \psi_t(y_1, y_2, \ldots, y_m),\ t = 1, 2.$$

Note that

$$I_\phi(h_1, h_2, \ldots, h_n) = I_{\psi_1}(h_1, h_2, \ldots, h_n) \cap I_{\psi_2}(h_1, h_2, \ldots, h_n).$$

Obviously

$$\prod_{i\in I} R_i/\mathcal{T} \models \phi(h_1\mathcal{T}, h_2\mathcal{T}, \ldots, h_n\mathcal{T})$$

if and only if $I_{\psi_1}, I_{\psi_2} \in \mathcal{T}$, which is equivalent to $I_\phi = I_{\psi_1} \cap I_{\psi_2} \in \mathcal{T}$.

Now we consider the case $\phi = (\exists y)\psi$. We suppose that our statement is proved for ψ. For simplicity we assume that $\psi = \psi(y, y_1, y_2, \ldots, y_n)$. Clearly

$$\prod_{i\in I} R_i/\mathcal{T} \models \phi(h_1\mathcal{T}, h_2\mathcal{T}, \ldots, h_n\mathcal{T})$$

if and only if

$$\prod_{i\in I} R_i/\mathcal{T} \models \psi(h\mathcal{T}, h_1\mathcal{T}, h_2\mathcal{T}, \ldots, h_n\mathcal{T})$$

for some $h \in \prod_{i\in I} R_i$. The last is equivalent to

$$I_\psi(h, h_1, h_2, \ldots, h_n) \in \mathcal{T}.$$

So it is enough to prove that $I_\phi(h_1, h_2, \ldots, h_n) \in \mathcal{T}$ if and only if $I_\psi(h, h_1, h_2, \ldots, h_n) \in \mathcal{T}$ for some $h \in \prod_{i\in I} R_i$. The "if" part is clear since

$$I_\phi(h_1, h_2, \ldots, h_n) \supseteq I_\psi(h, h_1, h_2, \ldots, h_n).$$

Suppose that $J = I_\phi(h_1, h_2, \ldots, h_n) \in \mathcal{T}$. Then there exist elements r_j, $j \in J$, such that

$$R_j \models \psi(r_j, h_1(j), h_2(j), \ldots, h_n(j)).$$

Define the element $h \in \prod_{i\in I} R_i$ by setting $h(j) = r_j$,$h(i) = 0$ for all $j \in J$, $i \in I \setminus J$. Clearly $I_\psi(h, h_1, h_2, \ldots, h_n) \supseteq J$. Thus $I_\psi(h, h_1, \ldots, h_n) \in \mathcal{T}$.

Since any formula is equivalent to a formula containing only atomic formulas, symbols $\neg$, $\wedge$, $\exists$, variables and bracket symbols, the theorem is proved (see Corollary 1.5.4).

Chapter 2

Rings of Quotients

2.1 Maximal Right Rings of Quotients

In the study of generalized identities in prime and semiprime rings it will be seen that rings of quotients play a crucial role. Not only will we want to extend generalized identities to rings of quotients, but the very presence of a suitable ring of quotients is necessary in order to properly define a generalized identity. For us the most important ring of quotients is the so called symmetric ring of quotients but at times we will want to employ the more general maximal ring of quotients.

For S a subset of R the left annihilator $\{x \in R \mid xS = 0\}$ will be denoted by $l_R(S)$ or simply $l(S)$ when the context is clear. The right annihilator $r_R(S)$ is similarly defined. A right ideal J of R is *dense* if given any $0 \neq r_1 \in R$, $r_2 \in R$ there exists $r \in R$ such that $r_1 r \neq 0$ and $r_2 r \in J$. One defines a dense left ideal in an analogous fashion. The collection of all dense right ideal of R will be denoted by $\mathcal{D} = \mathcal{D}(R)$. For any submodule J of a right R-module M and any subset $S \subseteq M$ we set

$$(S : J)_R = \{x \in R \mid Sx \subseteq J\}.$$

When the context is clear we will simply write $(S : J)$.

Although occasionally a result may hold for arbitrary rings, we shall assume throughout this section that R is a semiprime ring.

Proposition 2.1.1 *Let $I, J, S \in \mathcal{D}(R)$ and let $f : I \to R$ be a homomorphism of right R-modules. Then:*

(i) *$f^{-1}(J) = \{a \in I \mid f(a) \in J\} \in \mathcal{D}(R)$;*

(ii) *$(a : J) \in \mathcal{D}(R)$ for all $a \in R$;*

(iii) *$I \cap J \in \mathcal{D}(R)$;*

(iv) *If K is a right ideal of R and $K \supseteq I$, then $K \in \mathcal{D}(R)$;*

(v) *$l(I) = 0 = r(I)$;*

(vi) *If K is a right ideal of R and $(a : K) \in \mathcal{D}(R)$ for all $a \in I$, then $K \in \mathcal{D}(R)$;*

(vii) *If L is a right ideal of R and $g : L \to R$ is a homomorphism of right S-modules, then g is a homomorphism of right R-modules;*

(viii) *$IJ \in \mathcal{D}(R)$.*

Proof. **(i)** Let $r_1 \neq 0$, $r_2 \in R$. Since I is a dense right ideal of R, $r_1r' \neq 0$ and $r_2r' \in I$ for some $r' \in R$. Analogously $(r_1r')r'' \neq 0$ and $f(r_2r')r'' \in J$ for some $r'' \in R$. Setting $r = r'r''$ we conclude that $r_1r \neq 0$ and $r_2r \in f^{-1}(J)$, which means that $f^{-1}(J)$ is a dense right ideal of R.

(ii) Letting l_a denote the left multiplication by a we note that $(a : J) = l_a^{-1}(J)$. Now apply **(i)**.

(iii) If i is the inclusion map $I \to R$, then $I \cap J = i^{-1}(J)$. Now apply **(i)**.

(iv) Is obvious.

(v) Suppose $Ia = 0$ for some $0 \neq a \in R$. Setting $r_1 = a = r_2$ we see that there exists $r \in R$ such that $0 \neq ar \in I$. We then have a contradiction $arRar \subseteq Iar = 0$. Next we suppose $l(I) \neq 0$. Since R is semiprime, there exist $a, b \in l(I)$ such that $ab \neq 0$. Now we can find $r \in R$ such that $abr \neq 0$ and $br \in I$. But $abr \in aI = 0$ and again a contradiction is reached.

(vi) Let $0 \neq r_1, r_2 \in R$. Since $I \in \mathcal{D}$, there is an element $r' \in R$ such that $r_1 r' \neq 0$ and $r_2 r' \in I$. Hence $(r_2 r' : K) \in \mathcal{D}$. By part **(v)** we then have $l\left((r_2 r' : K)\right) = 0$ and hence $r_1 r' r'' \neq 0$ and $r_2 r' r'' \in K$ for some $r'' \in (r_2 r' : K)$. Thus $K \in \mathcal{D}$.

(vii) Let $x \in L$ and $r \in R$. By *(ii)* $(r : S)_R \in \mathcal{D}$ and so by **(iii)** $M = (r : S)_S \cap S \in \mathcal{D}$. For every $y \in M \subseteq S$ we have $ry \in S$ and so

$$(g(xr) - g(x)r)y = g(xr)y - g(x)(ry) = g(xry) - g(xry) = 0.$$

It follows from **(v)** that $g(xr) = g(x)r$ and thus g is a homomorphism of right R-modules.

(viii) Let $r_1 \neq 0$ and $r_2 \in R$. By **(ii)** $L = (r_2 : I) \in \mathcal{D}(R)$, and so by (v) there exist $r' \in L$ such that $r_1 r' \neq 0$ and $r'' \in J$ such that $r_1 r' r'' \neq 0$. Setting $r = r' r''$ we then have $r_1 r \neq 0$ and $r_2 r = (r_2 r') r'' \in IJ$.

As an alternate definition of dense right ideal we have

Corollary 2.1.2 *Let J be a right ideal of R. Then $J \in \mathcal{D}$ if and only if $l_R\left((a : J)\right) = 0$ for all $a \in R$.*

Proof. If $J \in \mathcal{D}$ we know from Proposition 2.1.1**(ii)** and **(v)** that $(a : J) \in \mathcal{D}$ and $l_R\left((a : J)\right) = 0$. Conversely, given $r_1 \neq 0$, $r_2 \in R$ we know that $r_1(r_2 : J) \neq 0$, and so we may choose $r \in (r_2 : J)$ such that $r_1 r \neq 0$. But since $r \in (r_2 : J)$, we also have $r_2 r \in J$.

At this point we pause to mention the notion of essential right ideal. We recall that a right ideal J of R is *essential* if for every nonzero right ideal K of R we have $J \cap K \neq 0$. This notion may perhaps strike the reader as a more familiar and more natural one than that of a dense right ideal, but it does have the drawback that (even for primitive rings) the left annihilator of an essential right ideal may not be 0. A more through discussion of the relationship between essential and dense right ideals will be given at the end of this section. For now we have the following remark.

Remark 2.1.3 *Let J be a dense right ideal of R. Then J is an essential right ideal of R.*

Proof. Indeed, for $0 \neq a \in R$, pick $r \in R$ such that $0 \neq ar \in J$. Then $0 \neq ar \in J \cap aR$.

There is one prominent situation, however, when the two notions coincide, and we leave it for the reader to verify the following

Remark 2.1.4 *Let I be a 2-sided ideal of R. Then the following conditions are equivalent:*

(i) *$l(I) = 0$;*

(ii) *I is a dense right ideal;*

(iii) *I is an essential right ideal;*

(iv) *I is essential as a 2-sided ideal (i.e., for any ideal $J \neq 0$, $I \cap J \neq 0$).*

Because of the symmetry imposed by **(iv)** the words "left" and "right" may be interchanged. In case R is prime an ideal is essential if and only if it is nonzero. For semiprime rings we have the following result and we again leave it for the reader to verify the straightforward details of its proof.

Remark 2.1.5 *Let I be a 2-sided ideal of R. Then:*

(i) *$l(I) = r(I)$;*

(ii) *$l(I) \cap I = 0$;*

(iii) *$I + l(I)$ is a dense right ideal of R.*

We continue now with our discussion of dense right ideals, pointing out the following useful properties.

Remark 2.1.6 *Let J be a right ideal of R and let $f : J \to R$ be a right R-module homomorphism. Then:*

(i) if $a \in R$ and $r(a) \in \mathcal{D}(R)$, then $a = 0$;

(ii) if $\ker(f) \in \mathcal{D}(R)$, then $f = 0$.

Proof. The first statement follows from Proposition 2.1.1(**v**). Suppose that $\ker(f) \in \mathcal{D}(R)$. Then we have $f(b)(b : \ker(f)) = 0$ for all $b \in J$. According to Proposition 2.1.1(**ii**), $(b : \ker(f)) \in \mathcal{D}(R)$. By the first statement we then have $f(b) = 0$. Thus $f = 0$.

We are now in a position to construct the desired ring of quotients of R. Consider the set

$$\mathcal{H} = \{(f;\, J) \mid J \in \mathcal{D}(R),\ f : J_R \to R_R\}.$$

We define $(f;\, J) \sim (g;\, K)$ if there exists $L \subseteq J \cap K$ such that $L \in \mathcal{D}$ and $f = g$ on L. One readily checks that $\sim$ is indeed an equivalence relation, and we let $[f;\, J]$ denote the equivalence class determined by $(f;\, J) \in \mathcal{H}$. We then define addition and multiplication of equivalence classes as follows (roughly speaking, just ordinary addition and composition of functions restricted to appropriate domains):

$$[f;\, J] + [g;\, K] = [f + g;\, J \cap K] \tag{2.1}$$

$$[f;\, J]\,[g;\, K] = \left[fg;\, g^{-1}(J)\right] \tag{2.2}$$

First of all we note that by Proposition 2.1.1 $J \cap K \in \mathcal{D}$ and $g^{-1}(J) \in \mathcal{D}$. One easily checks that addition is well-defined. We will show that multiplication is also well-defined. If $(f_1;\, J_1) \sim (f_2;\, J_2)$ and $(g_1;\, K_1) \sim (g_2;\, K_2)$ we may find $L \in \mathcal{D}$ such that $L \subseteq J_1 \cap J_2$, $f_1 = f_2$ on L and $M \in \mathcal{D}$ such that $M \subseteq K_1 \cap K_2$, $g_1 = g_2$ on M. Set $N = g_1^{-1}(L) \cap M$, and let $x \in N$. Then $N \in \mathcal{D}$ and

$$f_1 g_1(x) = f_1(g_1(x)) = f_1(g_2(x)) = f_2(g_2(x))$$

(noting that $g_1(x) = g_2(x) \in L$). Thus (2.2) is well-defined. We leave it for the reader to verify that the ring axioms holds, and so our construction is complete.

We shall denote the ring just constructed by $Q_{mr} = Q_{mr}(R)$ and shall call it the *maximal right ring of quotients* of R. It was first constructed by Utumi [270], and although there are more "homological" constructions of it available (see, e.g., [155]) we have preferred Utumi's very simple and natural construction using "partial" homomorphisms (indeed, speaking very loosely, given $f : J_R \to R_R$ and $fa = r$, $a \in J$, $r \in R$ we may "solve" for f and get "$f = ra^{-1}$" which says in some sense that f is a "fraction").

We proceed by showing that Q_{mr} is characterized by certain reasonable properties that any ring of quotients should have. First there is a ring injection $\beta : R \to Q_{mr}$ given by $a^\beta = [l_a;\, R]$, where l_a is the left multiplication determined by a. Secondly, given $q = [f;\, J] \in Q_{mr}$ one sees that $[f;\, J][l_a;\, R] = [l_{f(a)};\, R]$ for all $a \in J$, i.e., $qJ^\beta \subseteq R^\beta$. Thirdly, if $q = [f;\, J] \in Q_{mr}$ and $K \in \mathcal{D}$ such that $qK^\beta = 0$ then $q = 0$. Indeed, we have $0 = [f;\, J][l_a;\, R] = [l_{f(a)};\, R]$ for all $a \in J \cap K$ forcing $f(a) = 0$, whence $f(J) = 0$ and $q = 0$ (see Remark 2.1.6). Finally, suppose we are given a homomorphism of right R-modules $f : J_R \to R_R$, $J \in \mathcal{D}$. Then $[f;\, J][l_a;\, R] = [l_{f(a)};\, R]$ for all $a \in J$, i.e., $qa^\beta = f(a)^\beta$ for all $a \in J$, where $q = [f;\, J]$.

In a similar fashion, using the filter of dense left ideals $\mathcal{D}_l$, one can construct the maximal left ring of quotients $Q_{ml} = Q_{ml}(R)$ (in so doing it is best to put mappings on the right and use $(J;\, f)$ instead of $(f;\, J)$). One then embeds R into Q_{ml} via $\alpha : a \mapsto [R;\, r_a]$ and goes on to show an analogous set of properties holds for Q_{ml}. However, we are not interested in pursuing further the relationship between Q_{mr} and Q_{ml}; in any given situation we will just be working with one of them. For this reason we shall simplify matters by replacing R by its isomorphic image R^β in Q_{mr}, i.e., R is contained in Q_{mr}. We then summarize the four properties derived in the preceding paragraph.

Proposition 2.1.7 *$Q_{mr}(R)$ satisfies:*

(i) *R is a subring of Q_{mr};*

(ii) *For all $q \in Q_{mr}$ there exists $J \in \mathcal{D}$ such that $qJ \subseteq R$;*

(iii) *For all $q \in Q_{mr}$ and $J \in \mathcal{D}$, $qJ = 0$ if and only if $q = 0$;*

(iv) *For all $J \in \mathcal{D}$ and $f : J_R \to R_R$ there exists $q \in Q_{mr}$ such that $f(x) = qx$ for all $x \in J$.*

*Furthermore, properties **(i)**-**(iv)** characterize ring $Q_{mr}(R)$ up to isomorphism.*

Proof. We have only to prove the last statement. Let $Q \supseteq R$ be a ring having properties **(i)**-**(iv)**. Define the mapping $\alpha : Q \to Q_{mr}$ by the rule $q^\alpha = [l_q; (q : R)_R]$. One can readily check that α is an isomorphism of rings identical on R.

As a useful corollary to Proposition 2.1.7 we have

Lemma 2.1.8 *Given $q_1, q_2, \ldots, q_n \in Q_{mr}$ and $I, J \in \mathcal{D}(R)$ there exists $L \in \mathcal{D}(R)$ such that $L \subseteq J$ and $q_iL \subseteq I$ for all $i = 1, 2, \ldots, n$.*

Proof. Setting $J_i = (q_i : R)_R$ we note that $J_i \in \mathcal{D}$ for all i. Consider the map $f_i = l_{q_i} : J_i \to R_R$. By Proposition 2.1.1

$$K_i = f_i^{-1}(I) = \{x \in J_i \mid q_ix \in I\} \in \mathcal{D}.$$

Setting $L = (\cap_{i=1}^n K_i) \cap J$, we have the desired dense right ideal.

Lemma 2.1.9 *Let K be a dense right ideal of a semiprime ring R and S a subring of $Q_{mr}(R)$ such that $K \subseteq S$. Then:*

(i) *S is a semiprime ring;*

(ii) *A right ideal J of S is dense if and only if $(J \cap R)K \in \mathcal{D}(R)$ (in particular $IS \in \mathcal{D}(S)$ if $I \in \mathcal{D}(R)$);*

(iii) *A right ideal J of S is essential if and only if $(J \cap R)K$ is an essential right ideal of R.*

Proof. **(i)** Assume that I is a nonzero nilpotent ideal of S and pick $0 \neq q \in I$. By Proposition 2.1.7(**ii**), $qJ \subseteq R$ for $J \in \mathcal{D}(R)$ and by Proposition 2.1.7(**iii**) $0 \neq q(J \cap K) \subseteq I \cap R$ is a nonzero nilpotent right ideal of the semiprime ring R, a contradiction.

(ii) Suppose that $J \in \mathcal{D}(S)$ and $r_1 \neq 0$, $r_2 \in R$. Since $K \in \mathcal{D}(R)$, $L = (r_1 : K)_R \cap (r_2 : K)_R \in \mathcal{D}(R)$. By Proposition 2.1.1(**v**), $r_1r' \neq 0$ for some $r' \in L$. Clearly $r_1r', r_2r' \in K \subseteq S$. Therefore there exists an element $q \in S$ such that $r_1r'q \neq 0$ and $r_2r'q \in J$. Again by Proposition 2.1.1 we have that $r_1r'qr'' \neq 0$ for some $r'' \in (q : R)_R \cap K$. Clearly $r_2r'qr'' \in J \cap R$. Pick $r''' \in K$ such that $r_1r'qr''r''' \neq 0$. Since $r_2r'qr''r''' \in (J \cap R)K$ and $r'qr''r''' \in R$, we conclude that $(J \cap R)K \in \mathcal{D}(R)$.

Conversely, let $(J \cap R)K \in \mathcal{D}(R)$ and $s_1 \neq 0$, $s_2 \in S$. According to Proposition 2.1.1 we have $s_1r' \neq 0$ for some

$$r' \in (s_1 : R)_R \cap (s_2 : R)_R \cap K.$$

Clearly $s_1r', s_2r' \in R$ and $r' \in K \subseteq S$. Since $(J \cap R)K \in \mathcal{D}(R)$, $(s_2r' : (J \cap R)K)_R \in \mathcal{D}(R)$ and therefore

$$L = (s_2r' : (J \cap R)K)_R \cap K \in \mathcal{D}(R).$$

Hence there exists an element $r'' \in L$ such that $s_1r'r'' \neq 0$. Note that $s_2r'r'' \in (J \cap R)K \subseteq J$ and $r', r'', r'r'' \in K \subseteq S$. Therefore J is a dense right ideal of S. In particular, if $I \in \mathcal{D}(R)$, then $(IS \cap R)K \supseteq (IK \cap R)K \supseteq IK^2$, and so $IS \in \mathcal{D}(S)$.

(iii) Assume that J is an essential right ideal of S. We set $I = J \cap R$. Let M be any nonzero right ideal of R. By Remark 2.1.3 K is an essential right ideal of R and so $M \cap K \neq 0$. Then $(M \cap K)S$ is a nonzero right ideal of S, since S is semiprime and so $l_S(S) = 0$. Then $(M \cap K)S \cap J \neq 0$. Let $0 \neq q = \sum_{i=1}^{n} k_iq_i \in (M \cap K)S \cap J$, where $k_i \in M \cap K$ and $q_i \in S$. By Lemma 2.1.8, $q_iL \in R$ for some dense right ideal $L \subseteq K$ of R, $i = 1, 2, \ldots, n$. Obviously $0 \neq qL \in M \cap (J \cap R)$

and so $0 \neq qLK \in M \cap ((J \cap R)K)$. Therefore $(J \cap R)K$ is an essential right ideal of R.

Conversely, let $(J \cap R)K$ be an essential right ideal of R and let P be a nonzero right ideal of S. Choosing $0 \neq p \in P$ we see from Lemma 2.1.8 that $pL \subseteq K$ for some $L \subseteq K$, $L \in \mathcal{D}(R)$. Then $P \cap R \neq 0$, $(P \cap R)K \neq 0$ and hence $J \cap P \supseteq (J \cap R)K \cap (P \cap R)K \neq 0$. Thus $J \cap P \neq 0$ and the proposition is proved.

Proposition 2.1.10 *Let K be a dense right ideal of R and S a subring of $Q_{mr}(R)$ such that $K \subseteq S$. Then $Q_{mr}(S) = Q_{mr}(R)$.*

Proof. We verify the four properties of Proposition 2.1.7. Since $S \subseteq Q_{mr}(R)$, **(i)** holds. Let $q \in Q_{mr}(R)$. By Lemma 2.1.8, $qI \subseteq K$ for some $I \in \mathcal{D}(R)$, $I \subseteq K$. According to Lemma 2.1.9, $IS \in \mathcal{D}(S)$ and we have $qIS \subseteq KS \subseteq S$, thus proving **(ii)**. Next suppose $qJ = 0$ for some $q \in Q_{mr}(R)$, $J \in \mathcal{D}(S)$. By Lemma 2.1.9**(ii)** $(J \cap R)K \in \mathcal{D}(R)$ whence $q = 0$ and so **(iii)** is proved. Finally suppose we are given $f : J_S \to S_S$, $J \in \mathcal{D}(S)$. Setting

$$L = \{x \in (J \cap R)K \mid f(x) \in R\}$$

we shall show that $L \in \mathcal{D}(R)$ and $f : L \to R$ is a homomorphism of right R-modules. Note that $(J \cap R)K \in \mathcal{D}(R)$ by Lemma 2.1.9**(ii)**. Since $K \subseteq S$, f is a homomorphism of right K-modules and so by Proposition 2.1.1**(vii)** f is a homomorphism of right R-modules. It follows from Proposition 2.1.1**(i)** that $L = f^{-1}((J \cap R)K) \in \mathcal{D}(R)$. Thus there exists $q \in Q_{mr}(R)$ such that $f(x) = qx$ for all $x \in L$. We claim that $f(z) = qz$ for all $z \in J$. Indeed, by Lemma 2.1.9 $LS \in \mathcal{D}(S)$. Clearly $LS \subseteq J$ and $f(z) = qz$ for all $z \in LS$. Given any $z \in J$ and $s \in (z : LS)_S$ we have

$$(f(z) - qz)s = f(z)s - qzs = f(zs) - qzs = qzs - qzs = 0.$$

Since $(z : LS)_S \in \mathcal{D}(S)$, we conclude that $f(z) = qz$ for all $z \in J$, and **(vi)** has thereby been shown.

The following result is an immediate corollary of the above Proposition.

Theorem 2.1.11 *Let R be a semiprime ring and $Q = Q_{mr}(R)$. Then $Q_{mr}(Q) = Q$.*

Corollary 2.1.12 *Let R be a semiprime ring, I an ideal of R and $J = l_R(I)$. Then $Q_{mr}(R) = Q_{mr}(I) \oplus Q_{mr}(J)$.*

Proof. By Remark 2.1.5, $I \oplus J \in \mathcal{D}(R)$. According to Proposition 2.1.10, $Q_{mr}(R) = Q_{mr}(I \oplus J)$. Now our statement follows from the obvious equality $Q_{mr}(I \oplus J) = Q_{mr}(I) \oplus Q_{mr}(J)$.

For a ring R we set

$$Z_r(R) = \{x \in R \mid r_R(x) \quad \text{is an essential right ideal }\}.$$

We remark that $Z_r(R)$ is called the *(right) singular ideal* of R .

Lemma 2.1.13 *Let R be a semiprime ring, K an essential right ideal of R and $r \in R$. Then:*

(i) $(r : K)_R$ is an essential right ideal of R;

(ii) $Z_r(R)$ is an ideal of R;

(iii) $Z_r(R) = 0$ if and only if every essential right ideal is dense;

(iv) for any subring $R \subseteq S \subseteq Q_{mr}(R)$, $Z_r(R) = R \cap Z_r(S)$.

Proof. **(i)** Let $L \neq 0$ be a right ideal of R. If $rL = 0$, then $L \subseteq (r : K)$ and hence $0 \neq L = L \cap (r : K)$. Suppose that $rL \neq 0$. Since rL is a right ideal of R, $rL \cap K \neq 0$. But $rL \cap K = r[L \cap (r : K)]$. Therefore $L \cap (r : K) \neq 0$ and $(r : K)$ is essential.

(ii) Let $r_1, r_2 \in Z_r(R)$ and $x \in R$. Since $r_R(r_1 - r_2) \supseteq r_R(r_1) \cap r_R(r_2)$ and $r_R(r_1) \cap r_R(r_2)$ is an essential right ideal, $r_R(r_1 - r_2)$ is essential as well. Hence $r_1 - r_2 \in Z_r(R)$. Further as $r_R(xr_1) \supseteq r_R(r_1)$, $xr \in Z_r(R)$. By the above result the right ideal $(x : r_R(r_1))$ is essential. From $r_R(r_1x) \supseteq (x : r_R(r_1))$ it follows that $r_1x \in Z_r(R)$. Therefore $Z_r(R)$ is an ideal of R.

(iii) Suppose that $Z_r(R) = 0$. Let J be an essential right ideal of R. Taking into account **(i)**, we get $l_R((a : J)) = 0$ for all $a \in R$. By Corollary 2.1.2 we then have $J \in \mathcal{D}$. The converse statement follows from Proposition 2.1.1(**v**).

(iv) Note that $r_R(x) = r_S(x) \cap R$ for all $x \in R$ and so by Lemma 2.1.9 $r_R(x)$ is an essential right ideal of R if and only if $r_S(x)$ is an essential right ideal of S. Hence $Z_r(R) = Z_r(S) \cap R$.

Lemma 2.1.14 *Let R be a semiprime ring, $Q = Q_{mr}(R)$ and K a submodule of the right R-module Q. Suppose that $\alpha : K \to Q$ is a homomorphism of right R-modules. Then:*

(i) The rule $\widehat{\alpha}(\sum_{i=1}^n k_iq_i) = \sum_{i=1}^n \alpha(k_i)q_i$ where $k_i \in K$ and $q_i \in Q$ defines a homomorphism of right Q-modules $\widehat{\alpha} : KQ \to Q$;

(ii) If K is a right ideal of the ring Q, then α is a homomorphism of right Q-modules.

Proof. **(i)** It is enough to check that $\widehat{\alpha}$ is well-defined. Indeed, let $\sum_{i=1}^n k_iq_i = 0$ where $k_i \in K$, $q_i \in Q$. By Lemma 2.1.8 there exists a dense right ideal L of R such that $q_iL \subseteq R$ for all i. For any $x \in L$ we have

$$\left[\sum_{i=1}^n \alpha(k_i)q_i\right] x = \sum_{i=1}^n \alpha(k_i)(q_ix) = \alpha\left(\sum_{i=1}^n k_iq_ix\right) = 0.$$

Therefore $\sum_{i=1}^n \alpha(k_i)q_i = 0$ and $\widehat{\alpha}$ is well-defined.

(ii) If K is a right ideal of the ring Q, then $\alpha = \widehat{\alpha}$ which means that α is a homomorphism of right Q-modules.

Recall that a ring R is called *von Neumann regular* if for any $r \in R$ there exists an element $x \in R$ such that $rxr = r$. The following result is valid for arbitrary rings, but for simplicity we shall prove it only for semiprime rings.

Theorem 2.1.15 *Let R be a semiprime ring and $Q = Q_{mr}(R)$. Then the following conditions are equivalent:*

(i) Q is a von Neumann regular ring;

(ii) $Z_r(R) = 0$.

Furthermore, if the above conditions are fulfilled, then Q is an injective right R-module and Q-module.

Proof. Setting $Q = Q_{mr}(R)$, we suppose that Q is von Neumann regular. Let $0 \neq q \in Q$. Then $qxq = q$ for some $x \in Q$. Obviously $r_Q(xq) = r_Q(q)$ and $(xq)^2 = xq$. Hence $r_Q(xq) = (1 - xq)Q$. Since $(1 - xq)Q \cap xqQ = 0$, the right ideal $(1 - xq)Q$ is not essential. Therefore $Z_r(Q) = 0$. By Lemma 2.1.13, $Z_r(R) = 0$.

Conversely, let $Z_r(R) = 0$. Then by Lemma 2.1.13, the set $\mathcal{D}(R)$ coincides with the set of all essential right ideals of R. Let $q = [f;\, J] \in Q = Q_{mr}(R)$. We set $K = \ker(f)$. Choosing L to be a right ideal of R maximal with respect to the properties $L \subseteq J$ and $L \cap K = 0$, we note that $L \cong qL$. One can easily check that $K + L$ is an essential right ideal of R and hence $K + L \in \mathcal{D}(R)$. Now we choose M to be a right ideal of R maximal with respect to the property $M \cap qL = 0$. It is well known that $M \oplus qL$ is an essential right ideal of R. Hence $M \oplus qL \in \mathcal{D}(R)$. Define the mapping $g : M \oplus qL \to L$ by the rule $g(m + ql) = l$ for all $m \in M$, $l \in L$. Clearly $p = [g;\, M \oplus qL] \in Q$ and $fgf(k + l) = f(k + l)$ for all $k \in K$ and $l \in L$. Therefore $qpq = q$ and Q is von Neumann regular.

We show now that Q is an injective right R-module. Let K be a submodule of the right R-module Q and $\alpha : K \to Q$ a homomorphism of right R-modules. According to Lemma 2.1.14 we can assume that K is a right ideal of the ring Q and α is a homomorphism of right Q-modules. Choosing L to be a right ideal of Q maximal with respect to the property $L \cap K = 0$, we extend α up to homomorphism $\widehat{\alpha} : K + L \to Q$ by the rule $\widehat{\alpha}(k + l) = \alpha(k)$ for all $k \in K$, $l \in L$. Clearly $K + L$ is an essential right ideal of Q. Since $Z_r(Q) \cap R = Z_r(R) = 0$, we infer that $Z_r(Q) = 0$ (see Lemma 2.1.13 and Proposition 2.1.7). Then according to Lemma 2.1.13(**iii**), $K + L$ is a dense right ideal of Q. Hence $[\widehat{\alpha}; K + L] \in Q_{mr}(Q)$. Since $Q_{mr}(Q) = Q$ by Theorem 2.1.11, there exists an element $q \in Q$ such that $\widehat{\alpha} = l_q$ where l_q is left multiplication by q. Thus we have extended the mapping $\alpha : K \to Q$ up to an endomorphism of Q_Q. Applying this observation to the case $K \subseteq R$ we conclude that Q_R is an injective module. On the other hand, applying this observation to the case $K_Q \subseteq Q_Q$ we infer that Q_Q is an injective Q-module.

2.2 The Two-sided and Symmetric Rings of Quotients

The notion of two-sided rings of quotients (in which two-sided ideals are used) was introduced by W.S. Martindale [205] for prime rings (and extended to semiprime rings by Amitsur [8]). The construction of a two-sided ring of quotients is much simpler than of the maximal ring of quotients. Since the annihilator of any nonzero ideal of a prime ring is equal to zero, any nonzero ideal of a prime ring is dense and so the construction of the two-sided ring of quotients has an especially simple form for prime rings. We proceed to describe this construction for semiprime rings. In what follows R is a semiprime ring and

$$\mathcal{I} = \mathcal{I}(R) = \{I \mid I \quad \text{is an ideal of} \quad R \quad \text{and} \quad l(I) = 0\}.$$

We note that $\mathcal{I}$ is closed under products and finite intersections. We also mention that any $I \in \mathcal{I}$ is dense and essential as a right (or left) ideal and accordingly we shall call such ideals *dense* . Consider the set

$$\mathcal{T} = \{(f;\ J) \mid J \in \mathcal{I},\ f : J_R \to R_R\}$$

and define $(f;\ J) \simeq (g;\ K)$ if there exists $L \subseteq J \cap K$ such that $L \in \mathcal{I}$ and $f = g$ on L. We let $\{f;\ J\}$ denote the equivalence class determined by $(f;\ J) \in \mathcal{T}$. We now define addition and multiplication of equivalence classes as follows:

$$\begin{aligned} \{f;\ J\} + \{g;\ K\} &= \{f + g;\ KJ\} && (2.3) \\ \{f;\ J\}\{g;\ K\} &= \{fg;\ KJ\} && (2.4) \end{aligned}$$

We will only show that multiplication is well-defined. First of all we note that $KJ \in \mathcal{I}$ whenever $K, J \in \mathcal{I}$. Indeed, let $rKJ = 0$ for some $R \in R$. Then $rK \subseteq l(J) = 0$ and so $rK = 0$. Hence $r \in l(K) = 0$, $r = 0$ and $KJ \in \mathcal{I}$. Further $g(KJ) = g(K)J \subseteq J$ and so the composition fg is well-defined on KJ. If $(f_1;\ J_1) \simeq (f_2;\ J_2)$ and $(g_1;\ K_1) \simeq (g_2;\ K_2)$ we may find $L \in \mathcal{I}$ such that $L \subseteq J_1 \cap J_2$, $f_1 = f_2$ on L and $M \in \mathcal{I}$ such that $M \subseteq K_1 \cap K_2$, $g_1 = g_2$ on M. Set $N = ML$, and let $x \in N$. Then $N \in \mathcal{I}$ and

$$f_1g_1(x) = f_1(g_1(x)) = f_1(g_2(x)) = f_2(g_2(x))$$

(noting that $g_1(x) = g_2(x) \in L$). Thus (2.4) is well-defined. The reader can readily verify that the ring axioms hold, and so our construction is complete.

We shall denote the ring constructed above by $Q_r = Q_r(R)$ and shall call it the *two-sided right ring of quotients* of R .

We are now in a position to characterize the two-sided ring of quotients by its properties. First of all we note that the mapping $\gamma : R \to Q_r$ given by the rule $a^\gamma = \{l_a;\ R\}$ where l_a is the left multiplication determined by a, is a monomorphism of rings. Secondly, given $q = \{f;\ J\} \in Q_r$ and $a \in J$ one can easily check that $\{f;\ J\}\{l_a;\ R\} = \{l_{f(a)};\ R\}$, i.e., $qJ^\gamma \subseteq R^\gamma$. Thirdly, if $q = \{f;\ J\} \in Q_r$ and $K \in \mathcal{I}$ such that $qK^\gamma = 0$, then $q = 0$. Indeed, one sees that

$$\{f;\ J\}\{l_a;\ R\} = \{l_{f(a)};\ R\} = 0 \quad \text{for all} \quad a \in K \cap J$$

which means that $q = \{f;\ J\} = 0$. Finally, for any ideal $J \in \mathcal{I}$ and any given homomorphism $f : J_R \to R_R$, $J \in \mathcal{I}$, we have that $qa^\gamma = f(a)^\gamma$ where $a \in J$, $q = \{f;\ J\}$. We simplify matters by replacing R by its isomorphic image R^γ in Q_r, i.e., R is contained in Q_r, and summarize the four properties derived above.

Proposition 2.2.1 *Let R be a semiprime ring. Then $Q_r(R)$ satisfies:*

(i) R is a subring of Q_r;

(ii) For all $q \in Q_r$ there exists $J \in \mathcal{I}$ such that $qJ \subseteq R$;

(iii) For all $q \in Q_r$ and $J \in \mathcal{I}$, $qJ = 0$ if and only if $q = 0$;

(iv) For any ideal $J \in \mathcal{I}(R)$ and $f : J_R \to R_R$ there exists $q \in Q_r$ such that $f(x) = qx$ for all $x \in J$;

Furthermore, properties (i)-(iv) characterize ring $Q_r(R)$ up to isomorphism.

Proof. There remains only the last statement to prove. Let Q be a ring satisfying **(i)** – **(iv)**. For $q \in Q$, using **(i)** and **(ii)**, we define $q^\alpha = f;\ J$, where $qJ \subseteq R$, $J \in \mathcal{I}$, and $f(x) = qx$ for all $x \in J$. One readily checks that $\alpha : Q \to Q_r$ is a ring homomorphism. By **(iii)** α is an injection and by **(iv)** α is surjective, and so α is a ring isomorphism.

The next proposition describes the relation between $Q_{mr}(R)$ and $Q_r(R)$.

Proposition 2.2.2 *Given a semiprime ring R, there exists a unique ring monomorphism $\sigma : Q_r(R) \to Q_{mr}(R)$ such that $r^\sigma = r$ for all $r \in R$. Further,*

$$Im(\sigma) = \{q \in Q_{mr}(R) \mid qJ \subseteq R \quad \textit{for some} \quad J \in \mathcal{I}\}.$$

Proof. Define the mapping $\sigma : Q_r \to Q_{mr}$ by the rule $\{f;\, J\}^\sigma = [f;\, J]$ for all $\{f;\, J\} \in Q_r$. It follows directly from the definitions of $\sim$ and $\simeq$ that σ is well-defined. Obviously $r^\sigma = \{l_r;\, R\}^\sigma = [l_r;\, R] = r$ for all $r \in R$. Let $\{f;\, J\}, \{g;\, K\} \in Q_r$. Since $KJ \subseteq K \cap J$ and $KJ \in \mathcal{I}$, we have

$$\begin{aligned}(\{f;\, J\} + \{g;\, K\})^\sigma &= \{f+g;\, KJ\}^\sigma = [f+g;\, KJ] \\ &= [f;\, J] + [g;\, K]\end{aligned}$$

and σ is additive. Noting that $KJ \subseteq g^{-1}(J)$, one easily checks that σ preserve products. If $\{f;\, J\}^\sigma = 0$, then $f(L) = 0$ for some dense right ideal $L \subseteq J$. Then by Remark 2.1.6 $f = 0$ and therefore σ is a monomorphism. If $\sigma' : Q_r(R) \to Q_{mr}(R)$ is another ring monomorphism such that $r^{\sigma'} = r$ for all $r \in R$, then for every $q \in Q_r(R)$ and $x \in (q : R)_R$ we have

$$(q^\sigma - q^{\sigma'})x = q^\sigma x^\sigma - q^{\sigma'} x^{\sigma'} = (qx)^\sigma - (qx)^{\sigma'} = qx - qx = 0$$

and so $q^\sigma = q^{\sigma'}$ for all $q \in Q_r(R)$ thus proving the uniqueness.

We set

$$Q = \{q \in Q_{mr}(R) \mid qJ \subseteq R \quad \text{for some} \quad J \in \mathcal{I}\}.$$

Clearly $Im(\sigma) \subseteq Q$. Let $q \in Q$. Then $qJ \subseteq R$ for some $J \in \mathcal{I}$. We define $f : J \to R$ by the rule $f(x) = qx$ for all $x \in J$. Setting $q' = \{f;\, J\}^\sigma$, we note that $qa = q'a$ for all $a \in J$. Applying Proposition 2.1.7(**iii**), we infer that $q = q'$ and thus $Q = Im(\sigma)$.

In what follows we shall identify Q_r with Q via σ. We set

$$Q_s = \{q \in Q_{mr}(R) \mid qJ \cup Jq \subseteq R \quad \text{for some} \quad J \in \mathcal{I}\}.$$

One can easily check that Q_s is a subring of Q_r. We shall call it the *symmetric ring of quotients of R*. As noted by Passman ([236], Proposition 1.4) Q_s may be characterized by four properties analogous to those which characterize Q_{mr} (see Proposition 2.1.7).

Proposition 2.2.3 *Let R be a semiprime ring. Then $Q_s(R)$ satisfies:*

(i) *R is a subring of Q_s;*

(ii) *For all $q \in Q_s$ there exists $J \in \mathcal{I}$ such that $qJ \cup Jq \subseteq R$;*

(iii) *For all $q \in Q_s$ and $J \in \mathcal{I}$, $qJ = 0$ (or $Jq = 0$) if and only if $q = 0$;*

(iv) *Given $J \in \mathcal{I}$, $f : J_R \to R_R$ and $g : {}_RJ \to {}_RR$ such that $xf(y) = g(x)y$ for all $x, y \in J$, there exists $q \in Q$ such that $qx = f(x)$, $xq = g(x)$ for all $x \in J$.*

*Furthermore, properties **(i)**-**(iv)** characterize ring $Q_s(R)$ up to isomorphism.*

Proof. We leave for the reader the straightforward verification that Q_s enjoys the properties **(i)** – **(iv)**. Now assume that Q is a ring satisfying **(i)** – **(iv)**. We define a map $Q \to Q_{mr}$ by the rule $q \mapsto q' = [f;\, J]$, where J is given by **(ii)** and f is defined by $f(x) = qx$ for all $x \in J$. Again by **(ii)** one shows that for all $a \in J$

$$[l_a;\, R][f;\, J] = [l_af;\, J] = [l_{aq};\, J],$$

i.e. $aq' \in R$, whence $q' \in Q_s$. It is straightforward to show that $q \mapsto q'$ is a ring homomorphism. That $q \mapsto q'$ is an injection follows from property **(iii)**. Finally, given $p \in Q_s$ we have $pJ + Jp \subseteq R$ for some $J \in \mathcal{I}$. We then define $f : J_R \to R_R$ by $f(x) = px$ for all $x \in J$ and $g : {}_RJ \to {}_RR$ by $g(x) = xp$ for all $x \in J$. Thus $g(x)y = (xp)y = x(py) = xf(y)$ for all $x, y \in J$, and so by property **(iv)** there exists $q \in Q$ such that $qx = f(x)$, $xq = g(x)$ for all $x \in J$. Clearly $q' = p$ and so $q \mapsto q'$ is surjective. The proof of Proposition 2.2.3 is now complete.

We have defined Q_s as a subring of $Q_r \subseteq Q_{mr}$ and so, more accurately, we should have called Q_s the *right* symmetric ring of quotients of R. Analogously, the *left* symmetric ring of quotients Q'_s may be defined as a subring of $Q_l \subseteq Q_{ml}$. For $q \in Q_s$ we define $q' = J; g \in Q'_s$, where $xg = xq$ for all $x \in J$. Then the map $q \mapsto q'$ is an isomorphism of Q_s onto Q'_s (the key observation being that the map $l_a \to r_a$ is a ring homomorphism if one writes left multiplications on the left and right multiplications on the right). Thus we are able to make the following

Remark 2.2.4 *$Q_s \cong Q'_s$ (via the map defined above).*

2.3 The Extended Centroid

The center of the two-sided ring of quotients plays a key role in the definition of generalized identities. We will call the center $C = Z(Q_r)$ of the two-sided right ring of quotients Q_r of a semiprime ring R the *extended centroid of* R . We start our discussion of the extended centroid with the following obvious remark.

Remark 2.3.1 *Let R be a semiprime ring. Then*

$$Z(Q_s) = C = Z(Q_{mr}) = \{q \in Q_{mr} \mid qr = rq \quad \textit{for all} \quad r \in R\}.$$

Proof. If $c \in Z(Q_{mr})$, $x \in (c : R)_R$ and $r \in R$, then $c(rx) = r(cx) \in R$, $rx \in (c : R)_R$, and so $J = (c : R)_R$ is a dense ideal of R. Since $Jc = cJ \subseteq R$, $c \in Q_s$ and $Z(Q_{mr}) \subseteq Z(Q_s)$. According to Proposition 2.1.10, $Q_{mr}(Q_s) = Q_{mr}(R)$. Therefore $Z(Q_s) \subseteq Z(Q_{mr})$ and $Z(Q_s) = Z(Q_{mr})$. Analogously one can show that $Z(Q_r) = Z(Q_{mr})$.

If $q \in Q_{mr}$ and $qr = rq$ for all $r \in R$, then $(qx - xq)r = q(xr) - xqr = xrq - xrq = 0$ for all $x \in Q_{mr}$, $r \in (x : R)_R$. Thus $q \in C$.

Given a semiprime ring R, the subring RC of $Q_{mr}(R)$ is said to be the *central closure* of R. Further, R is called *centrally* *closed* if it coincides with its central closure (i.e., R is a C-subalgebra of Q_{mr}).

Next we prove the following important property of the extended centroid.

Theorem 2.3.2 *Let R be a semiprime ring, $Q = Q_{mr}(R)$, ${}_RU_R \subseteq {}_RQ_R$ a subbimodule of Q and $f : {}_RU_R \to {}_RQ_R$ a homomorphism of bimodules. Then there exists an element $\lambda \in C$ such that $f(u) = \lambda u$ for all $u \in U$.*

Proof. By Proposition 2.1.7, $W = U \cap R$ is a nonzero ideal of R. We set $I(w) = (f(w) : R)_R$ and $V = \sum_{w \in W} wI(w)$. Since $f(rw) = rf(w)$ for all $r \in R$ and $w \in W$, we have $f(rw)I(w) \subseteq R$ and $I(w) \subseteq I(rw)$. It follows that V is a left ideal of R. Hence, being a sum of right ideals, V is an ideal of R. Note that $f(V) = \sum f(w)(f(w) : R) \subseteq R$. Define a mapping $g : V \oplus r_R(V) \to R$ by the rule $g(v + v') = f(v) + v'$ for all $v \in V$, $v' \in r_R(V)$. Clearly g is a homomorphism of R-R-bimodules. Since $V \oplus r_R(V) \in \mathcal{D}(R)$, there exists an element $\lambda \in Q$ such that $g(x) = \lambda x$ for all $x \in V \oplus r_R(V)$. Note that

$$\lambda rx = g(rx) = rg(x) = r\lambda x \quad \text{for all} \quad x \in V \oplus r(V),\ r \in R.$$

Hence $r\lambda = \lambda r$ for all $r \in R$ and so $\lambda \in C$ by Remark 2.3.1. Further, let $u \in U$, $D = (u : R)_R$ and $d \in D$. Then for all $r \in (f(ud) : R)_R$ we have $udr \in V$ and

$$f(u)dr = f(udr) = g(udr) = \lambda udr,\ (f(u) - \lambda u)\,dr = 0.$$

Therefore $(f(u) - \lambda u)\,d = 0$ for all $d \in D$ and so $f(u) = \lambda u$ for all $u \in U$ (see Proposition 2.1.7(**iii**)). The proof is complete.

Now, using the above theorem and the Weak Density Theorem (Theorem 1.1.5), we will prove the following result. We consider Q as a left C-module. Then Q is a right $End_C(Q)$-module. Denote by $R_{(l)}$ ($R_{(r)}$) the subring of $End_C(Q)$ generated by all left (respectively, by all right) multiplications by elements of R and put $S = R_{(l)}R_{(r)} \subseteq End_C(Q)$.

Theorem 2.3.3 *Let R be a semiprime ring, $Q = Q_r(R)$, $C = Z(Q)$ and $q_1, q_2, \ldots, q_n \in Q$. Suppose that $q_1 \notin \sum_{i=2}^{n} Cq_i$. Then there exist an element $p = \sum_{i=1}^{m} l_{a_i} r_{b_i} \in R_{(l)}R_{(r)}$ such that*

$$q_1 \cdot p = \sum_{i=1}^{m} a_i q_1 b_i \neq 0 \quad \text{and} \quad q_j \cdot p = 0 \quad \text{for} \quad j \geq 2.$$

Proof. According to Theorem 2.3.2 Q is a closed right S-module and $C = End(Q_S)$. Setting $T = S$, $\Delta = C$ and $M = N = Q$, we note that T is a total S-submodule of the right S-module $Hom({}_\Delta M, {}_\Delta N) = End_C(Q)$. Indeed, for any $0 \neq q \in Q$ we have $qT = RqR \supseteq Rq(q : R)_R \neq 0$. Now apply Theorem 1.1.5.

For the convenience of the reader who is interested in the prime ring case only we will first prove the most important properties of the extended centroid of prime rings and then continue the discussion of the semiprime ring case.

The extended centroid of prime rings First of all we note that the extended centroid C of a prime ring R is a field. Indeed, let $0 \neq c \in C$. We shall show that c is invertible. Clearly $cU \subseteq R$ for some nonzero ideal U of R and cU is an ideal of R. Since any nonzero ideal of R is dense and the annihilator in R of a central element of Q is a two sided ideal, we infer from Proposition 2.2.1**(iii)** that $r_R(c) = 0$. Hence $cU_R \cong U_R$ and the mapping $f : cU \to U$ given by the rule $f(cu) = u$ for all $u \in U$ is well-defined. Letting t denote the element $\{f; cU\} \in Q$, we note that $tr = rt$ for all $r \in R$, and so by Remark 2.3.1, $t \in C$. Obviously $tcu = u$ for all $u \in U$ and so $tc = 1$.

Theorem 2.3.4 *Let R be a prime ring, $Q = Q_{mr}(R)$ and $a, b \in Q$. Suppose that $axb = bxa$ for all $x \in R$. Then a and b are C-dependent.*

Proof. If a, b are C-independent, then by Theorem 2.3.3 there exists an element $p = \sum_{i=1}^{m} l_{a_i} r_{b_i} \in R_{(l)}R(r)$ such that

$d = a \cdot p \neq 0$ and $b \cdot p = 0$. For all $r \in R$ we have

$$\begin{aligned} 0 &= ar\sum_{i=1}^{m} a_i b b_i = \sum_{i=1}^{m}(ara_i b)b_i \\ &= \sum_{i=1}^{m}(bra_i a)b_i = br\sum_{i=1} a_i a b_i = brd \end{aligned}$$

and $bRd = 0$. Choosing $x, y \in R$ such that $0 \neq bx \in R$ and $0 \neq dy \in R$ we conclude that $(bx)R(dy) = 0$ in contradiction to primeness of R. Thus a, b are C-dependent.

Theorem 2.3.5 *Let A be a centrally closed prime ring with extended centroid C and let B be any C-algebra such that $r_B(B) = 0 = l_B(B)$. Then any nonzero ideal W of the ring $A \otimes_C B$ contains a nonzero element of the form $a \otimes b$.*

Proof. Pick $0 \neq w \in W$ and write $w = \sum_{i=1}^{n} x_i \otimes y_i$ where we may assume without loss of generality that $x_1, x_2, \ldots, x_n$ are C-independent. We choose $p = \sum_{i=1}^{m} l_{a_i} r_{b_i} \in A_{(l)}A_{(r)}$ satisfying Theorem 2.3.3. Clearly $ry_1 s \neq 0$ for some $r, s \in B$. Then W contains the element

$$\sum_{i=1}^{m}(a_i \otimes r)w(b_i \otimes s) = \sum_j \sum_i a_i x_j b_i \otimes r y_j s = \sum_i a_i x_1 b_i \otimes r y_1 s \neq 0.$$

Theorem 2.3.6 *Let A be a centrally closed prime ring with extended centroid C and let A° be its opposite C-algebra. Then $A^\circ \otimes_C A \cong A_{(l)}A_{(r)} \subseteq End_C(A)$ under the mapping $a \otimes b \mapsto l_a r_b$ (here we regard $End_C(A)$ as acting from the right).*

Proof. By Remark 1.2.6 the mapping $\tau : A^\circ \otimes_C A \to A_{(l)}A_{(r)}$ given by the rule $\sum_i a_i \otimes b_i \mapsto l_{a_i} r_{b_i}$ is a well-defined surjective C-algebra map. Suppose that $\ker(\tau) \neq 0$. By Theorem 2.3.5 the ideal $\ker(\tau)$ contains a nonzero element of the form $a \otimes b$. Then $0 = \tau(a \otimes b) = l_a r_b$ and $aAb = A(l_a r_b) = 0$, a contradiction to the primeness of A. Therefore the mapping τ is an isomorphism.

Let R be a prime ring, $Q = Q_{mr}(R)$ and $a, b \in Q$. Suppose that $aRb = 0$. Then either $a = 0$, or $b = 0$. Indeed, let $a \neq 0$ and $b \neq 0$. Then $0 \neq ax \in R$ and $0 \neq by \in R$ for some $x, y \in R$. We have $(ax)R(by) = 0$, a contradiction to the primeness of R. Now we are in a position to prove the following generalization of Theorem 2.3.4.

Theorem 2.3.7 *Let R be a prime ring, $Q = Q_{mr}(R)$ and $q_i \in Q$, $1 \leq i \leq n$. Set $M = \sum_{i=1}^{n} Cq_i$. Then the following conditions are equivalent:*

(i) For all $r_1, r_2, \ldots, r_{n-1} \in R$

$$\sum_{\sigma \in S_n} \epsilon(\sigma) q_{\sigma(1)} r_1 q_{\sigma(2)} r_2 \ldots r_{n-1} q_{\sigma(n)} = 0, \tag{2.5}$$

where S_n is the permutation group;

(ii) $\dim_C(M) < n$.

Proof. To prove that **(i)** implies **(ii)** we proceed by induction on n. The case $n = 2$ follows from Theorem 2.3.4. Consider now the general case. Suppose that $q_n \notin \sum_{i=1}^{n-1} Cq_i$. Then by Theorem 2.3.3 there exists an element $p = \sum_{j=1}^{m} l_{a_j} r_{b_j} \in R_{(l)} R_{(r)}$ such that

$$q_n p = \sum_{j=1}^{m} a_j q_n b_j \neq 0 \quad \text{and} \quad q_i p = 0 \quad \text{for} \quad i < n.$$

Substituting in (2.5) $r_{n-1} a_j$ in place of r_{n-1} and multiplying by b_j from the right, we infer that

$$0 \; = \; \sum_{j=1}^{m} \sum_{\sigma \in S_n} \epsilon(\sigma) q_{\sigma(1)} r_1 q_{\sigma(2)} r_2 \ldots r_{n-1} a_j q_{\sigma(n)} b_j$$

$$= \sum_{\sigma\in S_n} \epsilon(\sigma)q_{\sigma(1)}r_1q_{\sigma(2)}r_2\ldots r_{n-1}\left(\sum_j a_jq_{\sigma(n)}b_j\right)$$

$$= \left(\sum_{\sigma\in S_{n-1}} \epsilon(\sigma)q_{\sigma(1)}r_1\ldots r_{n-2}q_{\sigma(n-1)}\right)r_{n-1}\left(\sum_j a_jq_nb_j\right)$$

for all $r_{n-1}\in R$ and so

$$\sum_{\sigma\in S_{n-1}} \epsilon(\sigma)q_{\sigma(1)}r_1q_{\sigma(2)}r_2\ldots r_{n-2}q_{\sigma(n-1)} = 0$$

for all $r_1, r_2, \ldots, r_{n-2}\in R$. Setting $M' = \sum_{i=1}^{n-1} Cq_i$, we infer from the induction hypothesis that $\dim_C(M') < n-1$. Thus

$$\dim_C(M) = \dim_C(M' + Cq_n) \leq n-2+1 < n.$$

The proof that **(ii)** implies **(i)** rests on the well-known argument that the standard polynomial vanishes on dependent vectors.

Let $Q = Q_{mr}(R)$ and $n > 0$. An element $a\in Q$ is called an *algebraic element of degree* $\leq n$ *over* C if there exists a polynomial $h(x) = x^n + c_1x^{n-1} + \ldots + c_n \in C[x]$ such that $h(a) = 0$. We set $a^0 = 1$.

Corollary 2.3.8 *Let R be a prime ring, $Q = Q_{mr}(R)$, $C = Z(Q)$ and $a\in Q$. Then the following conditions are equivalent:*

(i) a is an algebraic element of degree $\leq n$;

(ii) $\sum_{\sigma\in S_{n+1}} a^{\sigma(0)}r_0a^{\sigma(1)}r_1\ldots r_{n-1}a^{\sigma(n)} = 0$ for all $r_i\in R$.

The extended centroid of semiprime rings We begin with the following theorem which describes the properties of the extended centroid C of a semiprime ring R and the local structure of the C-module $Q_{mr}(R)$ as well.

Theorem 2.3.9 *Let R be a semiprime ring and $Q = Q_{mr}(R)$. Then:*

(i) For any subset $V \subseteq Q$ there exists a unique idempotent $E(V)$ such that $r_C(V) = (1 - E(V))C$; moreover $r_Q(QVQ) = (1 - E(V))Q$ and $E(V)v = v$ for all $v \in V$;

(ii) For any subset $V \subseteq Q$ and idempotent $e \in C$, $E(eV) = eE(V)$;

(iii) C is a von Neumann regular selfinjective ring (and hence $Q_{mr}(C) = C$);

(iv) Any finitely generated submodule $M = \sum_{i=1}^{n} Ca_i$ of the C-module Q contains a finite subset of nonzero elements $\{m_1, m_2, \ldots, m_k\}$, where k is the minimal number of generators of M, such that $M = \bigoplus_{i=1}^{k} Cm_i$ and $E(m_i)E(m_{i+1}) = E(m_{i+1})$ for all $i = 1, 2, \ldots, k-1$;

(v) Any finitely generated C-submodule M of Q is projective and injective.

Proof. **(i)** Letting I denote the ideal of $Q = Q_{mr}$ generated by the subset V, we note that $r_C(V) = r_C(I)$. Put $J = r_Q(I)$. According to Remark 2.1.5, $I \oplus J$ is a dense ideal of Q. Define the mapping $h : I \oplus J \to Q$ by the rule $h(i + j) = i$ for all $i \in I$, $j \in J$. Clearly $e = [h; I \oplus J] \in Q_{mr}(Q) = Q$ (see Theorem 2.1.11). We note also that $e^2 = e$ and $eq = qe$ for all $q \in Q$. Hence $e \in C$. We claim that $r_C(I) = (1 - e)C$. Indeed, let $c \in C$ be such that $Ic = 0$. Then $c(1 - e)(i + j) = cj = c(i + j)$ for all $i \in I$, $j \in J$. Since $I \oplus J$ is a dense ideal of Q, $c = c(1 - e)$ and $c \in (1 - e)C$. On the other hand the equality $(1 - e)I = 0$ implies that $r_C(I) \supseteq (1 - e)C$. Therefore $r_C(V) = r_C(I) = (1-e)C$. Being an identity element of the ring $(1 - e)C$, the element $1 - e$ (and so e) is uniquely determined. Note that $(1 - e)(I + J) = J$. Hence $r_Q(I) = J \subseteq (1 - e)Q$. On the other hand the inclusion $r_Q(I) \supseteq (1 - e)Q$ is obvious, since $eI = I$. Therefore $r_Q(I) = (1 - e)Q$.

(ii) Let $c \in r_C(eV)$. Since $ceV = 0$, $ce \in r_C(V) = (1 - E(V))C$ and so

$$c = ce + c(1 - e) \in (1 - E(V))C + (1 - e)C$$

and $r_C(eV) \subseteq (1 - E(V))C + (1 - e)C$. On the other hand $(1 - E(V))C + (1 - e)C \subseteq r_C(eV)$ and hence

$$\begin{aligned} r_C(eV) &= (1 - E(V))C + (1 - e)C \\ &= [1 - E(V) + 1 - e - (1 - E(V)(1 - e))]\, C \\ &= (1 - eE(V))C. \end{aligned}$$

Thus $E(eV) = eE(V)$.

(iii) Let $c \in C$ and $I = QcQ = Qc$. Setting $J = r_Q(I)$, we note that $I \oplus J$ is a dense ideal of Q. By Lemma 2.1.9, Q is a semiprime ring. Since c is a central element, $r_Q(c) = r_Q(c^2)$ and so $cQ_Q \cong c^2Q_Q$. In particular $r_Q(c^2Q) = r_Q(cQ) = J$. Hence $c^2Q \oplus J$ is a dense ideal of Q. Define the mapping $f : c^2Q \oplus J \to Q$ by the rule $f(c^2q + j) = cq + j$ for all $q \in Q$, $j \in J$. Clearly $t = [f; c^2Q \oplus J] \in Q_{mr}(Q) = Q$ and $tq = qt$ for all $q \in Q$. Hence $t \in C$. Since $ctc(cq + j) = c^2q = c(cq + j)$ for all $cq \in cQ$ and $j \in J$, $ctc = c$ and so C is von Neumann regular.

Now we show that C is selfinjective. Let K be an ideal of C and $f : K \to C$ a homomorphism of C-modules. It is enough to prove that there exists an element $c \in C$ such that $f(x) = cx$ for all $x \in K$. To this end we set $e = 1 - E(K)$ and note that $K \oplus eC$ is a dense ideal of C. By Zorn's Lemma K has a maximal subset D' of orthogonal idempotents. Setting $D = D' \cup \{e\}$, we claim that $r_C(D) = 0$. Indeed, if $r_C(D) \neq 0$, by **(i)** $r_C(D) = vC$ for some $0 \neq v = v^2 \in C$. Since $Dv = 0$ and $K + eC$ is a dense ideal of C, we infer that $Kv \neq 0$. Then $vk \neq 0$ and $vkyvk = vk$ for some $k \in K$, $y \in C$. Therefore $w = vky \in K$ is a nonzero idempotent orthogonal to all idempotents in D', a contradiction to the choice of D'. Hence $r_C(D) = 0$ and so by the above result $r_Q(QDQ) = 0$, which means that $L = DQ = QDQ$ is a dense ideal of Q and $DC = D'C + eC$ is a dense ideal of C as well. Clearly $L = \oplus_{d\in D} dQ$. Define the mapping $f' : L \to Q$ by the rule

$$f'\left(\sum_{d\in D} dq_d\right) = \sum_{d\in D'} f(d)q_d$$

where $q_d \in Q$ and only a finite number of q_d's are nonzero. Obviously $c = [f'; L] \in C$ and $f'(x) = cx$ for all $x \in L$. It follows immediately from the definition that $cx = f'(x) = f(x)$ for all $x \in D'C$. For $y \in K$, $d \in D'$ we then have $f(y)d' = f(d')y = cyd'$ and $f(y)e = f(ye) = 0$. It follows that $(cy - f(y))(DC) = 0$, whence $f(y) = cy$ for all $y \in K$, i.e. C is selfinjective.

(iv) First of all we note that given any $q \in Q$, the C-modules Cq and $CE(q)$ are isomorphic. Since $C = CE(q) \oplus C(1 - E(q))$, we conclude that Cq is an injective C-module.

We proceed by induction on n. The case $n = 1$ is obvious. Suppose that our statement is proved for $t < n$. Then the module $M' = \sum_{i=1}^{n-1} Ca_i$ contains a finite subset $m'_1, m'_2, \ldots, m'_{k'}$ of nonzero elements such that k' is the the minimal number of generators of M', $M' = \oplus_{i=1}^{k'} Cm'_i$ and $E(m'_i)E(m'_{i+1}) = E(m'_{i+1})$ for all $i = 1, 2, \ldots, k' - 1$. From the above observation it follows that M' is an injective C-module and so $M = M' \oplus N$ for some C-submodule N. Since $a_i \in M'$ for all $i \leq n - 1$, we infer that the module N is generated by the canonical projection a of a_n. We set

$$e_0 = 1,\ e_i = E(m'_i),\ m_i = m'_i + (e_{i-1} - e_i)a \quad \text{for } 1 \leq i \leq k',$$

$$k = \begin{cases} k' & \text{if } \ e_{k'}a = 0; \\ k' + 1 & \text{if } \ e_{k'}a \neq 0. \end{cases},$$

$$m_k = \begin{cases} m_{k'} & \text{if } \ k = k'; \\ e_{k'}a & \text{if } \ k \neq k'. \end{cases}.$$

One can easily check that $M = \oplus_{i=1}^{k} Cm_i$ and $Cm_i \cong Ce_i \oplus C(e_{i-1} - e_i)E(a)$. Hence $m_iC = (e_i + (e_{i-1} - e_i)E(a))\,C$ and

$E(m_i) = e_i + (e_{i-1} - e_i)E(a)$. We leave it for the reader to check that $E(m_i)E(m_{i+1}) = E(m_{i+1})$ for all $i = 1, 2, \dots, k-1$.

We show that k is the minimal number of generators of M. It was noted above that the mapping $\alpha : Cm_k \rightarrow CE(m_k)$ given by the rule $cm_k \mapsto cE(m_k)$ is an isomorphism of C-modules. Pick P to be a maximal ideal of C containing $1 - E(m_k)$. Clearly $E(m_k) \notin P$. Hence $PCE(m_k) \neq CE(m_k)$ and so $PCm_k \neq Cm_k$. Since $E(m_i)E(m_k) = E(m_k)$, $E(m_i) \notin P$ for all $i = 1, 2, \dots, k$. Therefore $PCm_i \neq Cm_i$ for all i. Taking into account the equality $PM = \oplus_{i=1}^{k} PCm_k$, we conclude that $M/PM \cong \oplus_{i=1}^{k} Cm_i/Pm_i$ and so M/PM is a k-dimensional linear space over the field C/P. Since any generating subset of the C-module M determines a generating subset of the vector space M/PM, we conclude that k is the minimal number of generators of M.

(v) By the above result $M = \oplus_i Cm_i$. Since $Cm_i \cong CE(m_i)$ and $CE(m_i)$ is a projective and injective C-module, we conclude that M is projective and injective.

Keeping the notations of Theorem 2.3.9(**iv**), we will call the number k the *dimension* of the C-module M and denote it by $\dim_C(M)$. The idempotents just introduced have the following useful property.

Lemma 2.3.10 *Let R be a semiprime ring, $Q = Q_{mr}(R)$ and S, T subsets of Q. Then the following conditions are equivalent:*

(i) $SIT = 0$ for some $I \in \mathcal{D}(R)$;

(ii) $TQS = 0$;

(iii) $E(S)T = 0$;

(iv) $E(T)E(S) = 0$.

Proof. **(i)** $\Rightarrow$ **(ii)** Consider $V = TQSI$. Clearly V is a submodule of the right R-module Q and $V^2 = 0$. Since R is a semiprime ring and $V \cap R$ is a nilpotent right ideal of R, we have $V \cap R = 0$. It follows from Proposition 2.1.7 that $TQS = 0$.

(ii) ⇒ (iii) Letting I denote the ideal of Q generated by the set S, we note that

$$T \subseteq l_Q(I) = r_Q(I) = (1 - E(S))Q$$

(see Theorem 2.3.9). It follows that $E(S)T \subseteq E(T)r_Q(I) = 0$.

(iii) ⇒ (iv) By Theorem 2.3.9 we have $0 = E(E(S)T) = E(S)E(T)$.

(iv) ⇒ (i) According to Theorem 2.3.9(**i**), $E(S)S = S$ and $E(T)T = T$. Hence

$$SRT = (E(S)S)\,A\,(E(T)T) = (E(S)E(T))\,SRT = 0.$$

Using the above results, we are now able to state and prove the analog of Theorem 2.3.4 for semiprime rings.

Theorem 2.3.11 *Let R be a semiprime ring, $Q = Q_{mr}(R)$, $a, b \in Q$ and $e = E(a)E(b)$. Suppose that $axb = bxa$ for all $x \in R$. Then there exists an invertible element $c \in C$ such that $ea = ceb$.*

Proof. Without loss of generality we can assume that $e \neq 0$. Suppose that $ea \notin (eb)C$. By Theorem 2.3.3 there exists an element $p = \sum_{i=1}^{m} l_{a_i} r_{b_i} \in R_{(l)}R(r)$ such that $d = (ea) \cdot p \neq 0$ and $(eb) \cdot p = 0$. Note that $eaxeb = e(axb) = ebxea$ for all $x \in R$. Further for all $r \in R$ we have

$$\begin{aligned} 0 &= ear\sum_{i=1}^{m} a_i ebb_i = \sum_{i=1}^{m}(eara_i eb)b_i \\ &= \sum_{i=1}^{m}(ebra_i ea)b_i = ebr\sum_{i=1} a_i eab_i = ebrd \end{aligned}$$

and $ebRd = 0$. Then $E(eb)d = 0$ by Lemma 2.3.10(**iii**). On the other hand $E(eb) = eE(b) = e$ by Theorem 2.3.9(**ii**). Hence

$$0 = ed = e\sum_{i=1}^{m} a_i eab_i = \sum_{i=1}^{m} a_i e^2 ab_i = \sum_{i=1}^{m} a_i eab_i = d,$$

a contradiction to $d \neq 0$. Therefore $ea \in (eb)C$ and $ea = c'eb$ for some $c' \in C$. Since $E(ea) = e$ and $r_C(ea) \supseteq r_C(c')$, we conclude that

$$(1-e)(1-E(c')) = 1-E(c'), \quad \text{and} \quad eE(c') = e$$

and so $E(ec') = e$. It follows that $r_C(ec' + 1 - e) = 0$. Since C is von Neumann regular, $c = ec' + 1 - c$ is invertible. Clearly $ceb = c'eb = ea$.

Corollary 2.3.12 *Let R be a semiprime ring with extended centroid C and $v = v^2 \in R$. Set $C_v = \{c \in C \mid cv \in R\}$. Then $Z(vRv) = C_v v$. In particular, if R is centrally closed, then $Z(vRv) = Cv$.*

Proof. Obviously $C_v v \subseteq Z(vRv)$. Let $d \in Z(vRv)$. Then $vd = d$ and $r_C(d) \supseteq r_C(v)$. It follows that $e = E(d)E(v) = E(d)$. For any $x \in R$ we have $vxd = (vxv)d = d(vxv) = dxv$ and so by Theorem 2.3.11 $d = ed = cev$ for some invertible element $c \in C$. Therefore $d \in C_v v$ and $Z(vRv) = C_v v$.

Theorem 2.3.13 *Let A be a centrally closed semiprime ring with extended centroid C and let A° be its opposite C-algebra. Then $A^\circ \otimes_C A \cong A_{(l)}A_{(r)} \subseteq End_C(A)$ under the mapping $a \otimes b \mapsto l_a r_b$.*

Proof. By Remark 1.2.6 the mapping $\tau : A^\circ \otimes_C A \to A_{(l)}A_{(r)}$ given by the rule $\sum_i a_i \otimes b_i \mapsto l_{a_i} r_{b_i}$ is a well-defined surjective C-algebra map. Suppose that $0 \neq \sum_{i=1}^n a_i \otimes b_i \in \ker(\tau)$. Consider the C-submodule $M = \sum_{i=1}^n Ca_i$. By Theorem 2.3.9 $M = \oplus_{j=1}^m Cd_j$ for some $d_1, d_2, \ldots, d_m \in M$. Since all a_i's are linear combinations of d_j's with coefficients in C, we can assume without loss of generality that $M = \oplus_{i=1}^n Ca_i$. Furthermore, since

$$a_i \otimes b_i = (a_i E(a_i)) \otimes (E(b_i)b_i) = (E(b_i)a_i) \otimes (E(a_i)b_i),$$

we can also assume that $E(a_i) = E(b_i)$ (see Theorem 2.3.9**(ii)**). By Theorem 2.3.3 there exists an element $p = \sum_{k=1}^{t} l_{u_k} r_{v_k} \in A_{(l)}A_{(r)}$ such that

$$a_1 p = \sum_{k=1}^{t} u_k a_1 v_k \neq 0 \quad \text{and} \quad a_i p = 0 \quad \text{for} \quad i \geq 2.$$

The inclusion $\sum_i a_i \otimes b_i \in \ker(\tau)$ is equivalent to the equality $\sum_i a_i x b_i = 0$ for all $x \in A$. Substituting $v_k x$ instead of x and multiplying by u_k from the left the above equality, we infer that

$$0 = \sum_{k=1}^{t} \sum_{i=1}^{n} u_k a_i v_k x b_i = \sum_i \left(\sum_k u_k a_i v_k \right) x b_i = (\sum_k u_k a_1 v_k) x b_1$$

for all $x \in A$. Taking into account that $E(b_1) = E(a_1)$ and $E(a_1)a_1 = a_1$, we infer from Lemma 2.3.10 that

$$0 = E(b_1) \sum_k u_k a_1 v_k = \sum_k u_k (E(b_1) a_1) v_k = \sum_k u_k a_1 v_k$$

a contradiction to $\sum_k u_k a_1 v_k \neq 0$. The proof is complete.

We close this section with the following useful result due to S. Montgomery [230].

Proposition 2.3.14 *Let R be a semiprime (prime) ring, $Q = Q_s(R)$, $0 \neq e^2 = e \in Q$ and $A = eQe \cap R$. Then A is a semiprime (respectively, prime) ring and $eQe = Q_s(A)$.*

Proof. Pick $I \in \mathcal{I}(R)$ such that $eI \cup Ie \subseteq R$. Letting $J = I^2$ we note that $eJe \subseteq R$ and so $eJe \subseteq A$. Suppose that $aAa = 0$ for some $a \in A$. In particular $aeJea = 0$. Since $ae = a = ea$, $aJa = 0$ and hence $(aJ)^2 = 0$. As R is semiprime, we conclude that $aJ = 0$ and so $a = 0$. Therefore A is semiprime. Suppose now that R is prime and $aAb = 0$ for some $a, b \in A$. Then again $aJb = 0$ and hence $(bRaJ)^2 = 0$. It follows that $bRa = 0$ and so either $a = 0$, or $b = 0$. Hence A is prime.

We claim that if $eqeIe = 0$, $q \in Q$, $I \in \mathcal{I}(R)$, then $eqe = 0$. Indeed, by Lemma 2.3.10 we have $eqe = eqeE(e) = 0$. As a corollary we see that if $I \in \mathcal{I}(R)$ such that $eIe \subseteq R$, then $eIe \subseteq I(A)$. Indeed, suppose $(eqe)(eIe) = 0$ for $eqe \in A$. Then by the above claim we have $eqe = 0$, which shows that $l_A(eIe) = 0$, i.e., $eIe \in \mathcal{I}(A)$.

We now proceed to show that $eQe = Q_s(A)$ by verifying the four properties **(i)** – **(iv)** of Proposition 2.2.3. Clearly $A \subseteq eQe$. Next, given $eqe \in eQe$, let $I \in \mathcal{I}(R)$ be such that eI, Ie, $eqeI$, $Ieqe$ are contained in R. Setting $J = I^2$, we see from the preceding paragraph that $eJe \in \mathcal{I}(A)$, and it is also clear that $(eqe)(eJe)$, $(eJe)(eqe)$ are contained in A, thus proving **(ii)**. Now suppose $eqeK = 0$ for some $K \in \mathcal{I}(A)$ and $0 \neq eqe \in eQe$. Pick $I \in \mathcal{I}(R)$ such that $eI \subseteq R$ and $Ieqe \subseteq R$ and set $J = I^2$. By the above claim $0 \neq eJeqe \subseteq A$. Thus $eJeqeK = 0$, a contradiction to $K \in \mathcal{I}(A)$, and so $eqe = 0$ and **(iii)** is proved.

To prove **(iv)** we are given mappings $f : K_A \to A_A$, $g : {}_AK \to {}_AA$, $K \in \mathcal{I}(A)$, such that $xf(y) = g(x)y$ for all $x, y \in K$. Our task is to find an element $eqe \in eQe$ for which $f(x) = eqex$ and $g(x) = xeqe$ for all $x \in K$. Again letting $J = I^2$, where $I \in \mathcal{I}(R)$ such that eI, Ie are contained in R, we set $U = JKJ$, $V = r_R(U)$ and note that $U + V \in \mathcal{I}(R)$. We define a map $F : U + V \to R$ by the rule:

$$\sum a_ik_ib_i + v \mapsto \sum f(ea_ik_i)b_i, \quad k_i \in K,\ a_i, b(i) \in J,\ v \in V$$

(using the fact that $ea_ik_i = (ea_ie)k_i \in AK \subseteq K$). To prove that F is well–defined suppose that $\sum a_ik_ib_i = 0$ and set $z = \sum f(ea_ik_i)b_i$. On the one hand $zE(e) = \sum f(ea_ik_i)eb_iE(e) = z$. On the other hand, for all reR,

$$\begin{aligned} zre &= \sum f(ea_ik_i)(eb_ire) = \sum f(ea_ik_ib_ire) \\ &= f\left(e\left[\sum a_ik_ib_i\right]re\right) = 0. \end{aligned}$$

By Lemma 2.3.10 $zE(e) = 0$ and so $z = 0$. Clearly F is a right R-module map and so there is an element $q \in Q_r$ such that

$q(u+v) = F(u+v)$, $u \in U$, $v \in V$. In particular $qak = f(eak)$, $a \in J$, $k \in K$, and $qv = 0$, $v \in V$.

From $qV = 0$ it is easy to see that $Vq = 0$. From $JKJV = 0$ we first obtain $KJV = 0$, whence from Lemma 2.3.10 we see that $Ke' = 0$, where $e' = E(V)$. Suppose $ee' \neq 0$. Choose $I \in \mathcal{I}(R)$ such that $ee'I$, Iee' are contained in R and set $L = I^2$. Then $ee'L \neq 0$ and so $0 \neq ee'Lee' \subseteq A$. But $Kee'Lee' = 0$, in contradiction to $K \in \mathcal{I}(A)$, and so $ee' = 0$, and with it $eV = 0$.

Next, for $k, l \in K$, $a, b \in J$, we see that

$$kaqbl = kaf(ebl) = kaef(ebl) = g(kae)ebl = g(kae)bl.$$

Thus $[kaq - g(kae)]bl = 0$ and, from the preceding paragraph, we then have $[kaq - g(kae)](U+V) = 0$, whence $kaq = g(kae)$. Therefore $q \in Q_s$. Then from

$$laf(k) = laef(k) = g(lae)k = laqk$$

we see that $U[f(k) - qk] = 0$ and, in view of the preceding paragraph, that $(U+V)[f(k) - qk] = 0$. Thus $f(k) = qk$, from which it follows that $f(k) = keqe$ for all $k \in K$. Similarly, one shows that $g(k) = keqe$ for all $k \in K$, and the proof is complete.

The most important properties of the extended centroid of prime rings and its key role in the definition of generalized identities of prime rings were discovered by W. S. Martindale [205]. Theorem 2.3.4 and Theorem 2.3.6 are taken from [205] (see also [214]). Regularity of extended centroids of semiprime rings was proved by S. Amitsur [8]. Other properties of extended centroids of semiprime rings were proved by K. I. Beidar [21]. Theorem 2.3.7 was proved in the more general situation of prime (not necessarily associative) Ω-rings by Yu. P. Razmyslov [247].

2.4 Rings of Quotients of Coproducts

Let $A = A_1 \coprod_K A_2$ be the coproduct of algebras A_1 and A_2 with 1 over a field K, with each $\dim_K(A_i) > 1$. By Corollary 1.4.11 we know that A is a prime ring. It is our purpose in the present section to prove that if each $\dim_K(A_i) > 2$ and at least one A_i is a domain, then $Q_s(A) = A$, i.e., A is equal to its own symmetric ring of quotients. This is a special case of far more general results but is the only result needed in this book (§7.4). For more general coproducts $R = R_1 \coprod_\Delta R_2$, where R_1 and R_2 are so-called Δ-rings with 1 over a division ring Δ, $Q_s(R)$ has also been determined (see [217], also [190], [215], [216], [223]).

For the time being we assume that $A = A_1 \coprod_K A_2$, A_1 and A_2 with 1 over a field K, with each $\dim_K(A_i) > 2$. We shall use the terminology and lemmas developed in section 1.4 and suggest the reader reacquaint himself with these matters. We let $Q = Q_s(A)$ denote the symmetric ring of quotients of A.

We fix a nonzero ideal I of A and let

$$Q_I = \{q \in Q \mid qI + Iq \subseteq A\}.$$

Next we fix $a \in I$ such that a is 0-pure of even height $n = |a| > 0$ and thus we may write $a = a_{12} + a_{21}$. For $q \in Q_I$, we let $b_q = qa$ and $c_q = aq$ (when the context is clear we will sometimes write $b = b_q$ and $c = c_q$). We have immediately the simple relationship

$$c_q a = ab_q, \quad q \in Q_I. \tag{2.6}$$

Since a is 0-pure of even height it follows easily from (2.6) and Lemma 1.4.10 that $|b_q| = |c_q| = m_q$. Clearly b_q is 0-pure if and only if c_q is 0-pure, and b_q is (i, j)-pure if and only if c_q is (i, j)-pure.

Lemma 2.4.1 *If $q \in Q_I$ is such that $m_q < n$, then $q = 0$.*

Proof. If $q \neq 0$, choose $r \in I$ such that $0 \neq rq \in A$. Therefore $rqa \neq 0$ (since a is 0-pure), whence $b = qa \neq 0$. We write $b = b_{1j} + b_{2j'}$, whence without loss of generality we may assume $b_{1j} \neq 0 \,(mod\, H^{m-1})$, where $m = m_q$. Now choose $y', y'' \in A_2$ such that y' and y'' are K-independent $mod\, H^0$ (this is possible since $\dim_K(A_2) > 2$). Setting $c' = ay'q \in A$, we see from $(ay'q)a = ay'(qa)$ that

$$c'a = ay'b. \tag{2.7}$$

It follows from (2.7) that $|c'| = m + 1$, and examination of the $(2, j)$-component of (2.7) yields

$$c'_{2j}aj'j \equiv a_{21}y'b_{1j} \,(mod\, H^{n+m}).$$

By Lemma 1.4.9 (we are assuming $m + 1 \leq n$) there exists $e_{j'1} \in H_{j'1}^{n-m-1}$ such that $a_{j'j} \equiv e_{j'1}y'b_{1j} \,(mod\, H^{n-1})$. Similarly there exists $f_{j'1}$ such that $a_{j'j} \equiv f_{j'1}y''b_{1j}$. It follows that $e_{j'1}y' \equiv f_{j'1}y''$. By Remark 1.4.8 we see in particular that $e_{j'1} \equiv 0$ (since y', y'' are K-independent $mod\, H^0$). This forces the contradiction $a_{j'j} \equiv 0$ and the lemma is proved.

Lemma 2.4.2 *If $q \in Q_I$ is such that $m_q > n$, then there exists $r \in A$ such that $m_{q-r} < m_q = m$.*

Proof. We let $b = b_q$ and write $b = b_{1j} + b_{2j'}$ (possibly $b_{1j} \equiv 0$ or $b_{2j'} \equiv 0$). Likewise we have $c = c_q = c_{1j} + c_{2j'}$. Examination of the (i, j)-component of $ca = ab$ shows that

$$c_{1j}a_{j'j} \equiv a_{12}b_{1j}. \tag{2.8}$$

Applying Lemma 1.4.9 to (2.8), we see in particular that $b_{1j} \equiv e_{1j}a_{j'j} \,(mod\, H^{m-1})$ for some $e_{1j} \in H_{ij}^{m-n}$. In exactly the same fashion $b_{2j'} \equiv f_{2j'}a_{jj'}$ for suitable $f_{2j'} \in H_{2j'}^{m-n}$. Setting $r = e_{1j} + f_{2j'}$ we have

$$\begin{aligned}(q-r)a &= b - ra \equiv b_{1j} + b_{2j'} - (e_{1j} + f_{2j'})(a_{jj'} + a_{j'j}) \\ &\equiv (b_{1j} - e_{1j}a_{j'j}) + (b_{2j'} - f_{2j'}a_{j'j}) \equiv 0 \,(mod\, H^{m-1}).\end{aligned}$$

In other words $m_{q-r} < m$ and the lemma is proved.

Lemma 2.4.3 *If $q \in Q_I$ is such that $m_q = m$ and i is given, then there exist $\lambda, \mu \in K$ such that $(q - \lambda)a \equiv \mu a_{ii'}$*

Proof. We write $b = b_q = b_{1j} + b_{2j'}$, $c = c_q = c_{1j} + c_{2j'}$. We may assume that $b_{12} \not\equiv 0$. From (2.8) we obtain $c_{12}a_{12} \equiv a_{12}b_{12}$ and application of Lemma 1.4.9 yields $b_{12} \equiv \alpha a_{12}$ for some $\alpha \in K$. Suppose $b_{21} \equiv 0$. Then

$$(q - \alpha)a = b - \alpha a \equiv b_{12} - \alpha(a_{12} + a_{21}) \equiv -\alpha a_{21}.$$

Also $qa = b \equiv b_{12} \equiv \alpha a_{12}$. Suppose that $b_{21} \not\equiv 0$, and hence $b_{21} \equiv \beta a_{21}$ for some $\beta \in K$. Then

$$(q - \alpha)a = b - \alpha a \equiv b_{12} + b_{21} - \alpha a_{12} - \alpha a_{21} \equiv (\beta - \alpha)a_{21}.$$

On the other hand

$$(q - \beta)a = b - \beta a \equiv b_{12} + b_{21} - \beta a_{12} - \beta a_{21} \equiv (\alpha - \beta)a_{12}.$$

The four cases just discussed show that the lemma has been proved.

With these lemmas to draw on we are now in a position to prove

Theorem 2.4.4 *Let $A = A_1 \coprod_K A_2$ be the coproduct of algebras A_1 and A_2 with 1 over a field K, with each $\dim_K(A_i) > 2$ and at least one of the A_i's a domain. Then $Q_s(A) = A$.*

Proof. We may assume that A_1 is a domain. Suppose there exists $q \in Q_s$ such that $q \notin A$. We have $qI + Iq \subseteq A$ for some nonzero ideal I of A, and we fix $a \in I$, a 0-pure of even height n. Repeated application of Lemma 2.4.2 (if necessary) together with Lemma 2.4.1 shows that we may assume without loss of generality that $m_q = n$, whence by Lemma 2.4.3 we may assume that $qa \equiv \mu a_{12}$, $\mu \in K$. In fact we may furthermore assume that $qa \equiv a_{12}$ (just replace q by $\mu^{-1}q$). It then follows from (2.6) that also $aq \equiv a_{12}$.

We claim now that $A_1 = K \oplus T_1$ where $T_1 = \{x \in A_1 \mid xq = 0\}$. Indeed, for $x \in A_1$ we see immediately that $|xqa| = |xa_{12}| \leq n$. In case $|xqa| < n$ the by Lemma 2.4.1 $xq = 0$ and we are finished. If $|xqa| = n$ then by Lemma 2.4.3 there exist $\alpha, \beta \in K$ such that $(xq - \alpha)a \equiv \beta a_{12} \equiv \beta qa$, i.e., $(xq - \alpha - \beta q)a \equiv 0\,(mod\, H^{n-1})$. By Lemma 2.4.1 again $xq - \alpha - \beta q = 0$, i.e., $(x - \beta)q = \alpha$. If $\alpha \neq 0$, we set $x_0 = \alpha^{-1}(x - \beta)$ and note that $x_0q = 1$. From this we obtain a contradiction $a = x_0qa = x_0a_{12} + \ldots$ (just compare the $(2,1)$-components of both sides). Therefore we are left with $\alpha = 0$ and accordingly $(x - \beta)q = 0$. This places $x - \beta \in T_1$, and so we have shown that $A_1 = K \oplus T_1$.

We next claim that $A_1 = K \oplus T_2$, where $T_2 = \{x \in A_1 \mid qx = x\}$. Indeed, since

$$a(1-q) = a - aq \equiv a_{12} + a_{21} - a_{12} \equiv a_{21},$$

the obvious analogue of the preceding claim may be invoked, with $1 - q$ playing the role of q.

Since $\dim_K(A_1) > 2$ and $A_1 = K \oplus T_1$, $T_1 \neq 0$. Choose $t_1 \neq 0$ in T_1 and let $t_2 \in T_2$. We see that $0 = t_1qt_2 = t_1t_2$ and by our assumption that A_1 is a domain we conclude that $T_2 = 0$. We therefore reach the contradiction that $A_1 = K$ and the theorem is proved.

2.5 Derivations and (Anti)automorphisms

Let R be a semiprime ring. We set $Q_{mr} = Q_{mr}(R)$, $Q_r = Q_r(R)$ and $Q_s = Q_s(R)$.

Proposition 2.5.1 *Any derivation δ of a semiprime ring R can be extended uniquely to a derivation of Q_{mr} (we shall let δ also denote its extension to Q_{mr}). Furthermore $Q_r^\delta \subseteq Q_r$ and $Q_s^\delta \subseteq Q_s$.*

Proof. Given any dense right ideal K of R, we set $K_\delta = \sum_{x\in K} x(x^\delta : K)_R$. Clearly $K_\delta \subseteq K$ is a right ideal of R and $(K_\delta)^\delta \subseteq K$. We claim that K_δ is a dense right ideal of R. Indeed, let $u, v \in R$ and $u \neq 0$. Since K is a dense right ideal of R, $vr \in K$ and $ur \neq 0$ for some $r \in R$. As we already know $((vr)^\delta : K)_R$ is a dense right ideal of R. Therefore $urr' \neq 0$ for some $r' \in ((vr)^\delta : K)_R$ (see Proposition 2.1.1). Clearly $vrr' \in K_\delta$ and so our claim is proved.

Let $q \in Q_{mr}$. Then $qJ \subseteq R$ for some $J \in \mathcal{D}(R)$. We define $f : J_\delta \to R$ by the rule $f(x) = (qx)^\delta - qx^\delta$ for all $x \in J_\delta$. For $r \in R$, $a \in J_\delta$ we have

$$\begin{aligned} f(ar) &= (qar)^\delta - q(ar)^\delta = ((qa)r)^\delta - q(ar)^\delta \\ &= (qa)^\delta r + (qa)r^\delta - qar^\delta - qa^\delta r = f(a)r. \end{aligned}$$

Therefore $[f; J_\delta] \in Q_{mr}$ and we define $q^\delta = [f; J_\delta]$. Hence $q^\delta \in Q_{mr}$, and so δ has been extended uniquely to an element δ of $End_Z(Q_{mr})$ such that

$$q^\delta a = (qa)^\delta - qa^\delta,\ (qa)^\delta = q^\delta a + qa^\delta \quad \text{for all} \quad a \in J_\delta. \qquad (2.9)$$

Note that $q^\delta J_\delta \subseteq R$.

Let $p, q \in Q_{mr}$. By Lemma 2.1.8 there exist dense right ideals J, I of R such that $pJ, qJ, pqJ \subseteq R$, $I \subseteq J_\delta$ and $qI \subseteq J_\delta$ as well. Then according to (2.9) we have

$$\begin{aligned} (pq)^\delta x &= (pqx)^\delta - pqx^\delta = p^\delta(qx) + p(qx)^\delta - pqx^\delta \\ &= (p^\delta q + pq^\delta)x \end{aligned}$$

for all $x \in I$. Hence $[(pq)^\delta - p^\delta q - pq^\delta]x = 0$ and so by Proposition 2.1.7 we have $(pq)^\delta - p^\delta q - pq^\delta = 0$. Therefore δ is a derivation of Q_{mr}.

Now let $q \in Q_r$. Then $qI \subseteq R$ for some dense ideal I of R. Clearly $(I^2)^\delta \subseteq I$. Letting J denote I^2, we conclude that $q^\delta J \subseteq (qJ)^\delta + qJ^\delta \subseteq R$ and so $q^\delta \in Q_r$.

Given any $q \in Q_s$, we have $qI + Iq \in R$ for some dense ideal I of R. We already know that $q^\delta \in Q_r$. Again for $J = I^2$ we infer that $Jq^\delta \subseteq (Jq)^\delta + J^\delta q \subseteq R$ and thus $q^\delta \in Q_s$. The proof is complete.

Let $Q \in \{Q_{mr}, Q_r, Q_s\}$. Proposition 2.5.1 enables us to regard $Der(R)$ as a Lie subring of $End_{\mathcal{Z}}(Q)$ where $\mathcal{Z}$ is the ring of integers. We may also regard C as contained in $End_{\mathcal{Z}}(Q)$ via the multiplication $x \mapsto cx$. $End_{\mathcal{Z}}(Q)$ becomes a C-ring according to $x^{tc} = cx^t$, $x \in Q$, $t \in End_{\mathcal{Z}}(Q)$, $c \in C$. If $\delta \in Der(Q)$, $c \in C$, and $x, y \in Q$, then

$$(xy)^{\delta c} = c(xy)^\delta = cx^\delta y + cxy^\delta = x^{\delta c}y + xy^{\delta c}$$

and so $\delta c \in Der(Q)$. Thus $Der(Q)$ is a submodule of the right C-module $End_{\mathcal{Z}}(Q)$ and in particular $(Der(R))C$ is a C-submodule of $Der(Q)$. It is important to point out that in general $c \in C$ does not commute with $\delta \in Der(Q)$, but we do have the commutation formula

$$c\delta = \delta c + c^\delta,\ c \in C,\ \delta \in Der(R). \tag{2.10}$$

We let $D_i = D_i(R)$ denote the inner derivations of Q, i.e., all derivations of Q of the form $ad(q)$, $q \in Q$. This is a (possibly) larger set of derivations than the set of *X-inner derivations* of R (so named by S. Montgomery in honor of Kharchenko), the latter being those of the form $ad(q)$ where $[R, q] \subseteq R$.

Remark 2.5.2 *Let $q \in Q_{mr}$ be such that $ad(q)$ is an X-inner derivation of R. Then $q \in Q_s$.*

Proof. Let $J = (q : R)_R$. Since $[R, q], qJ \subseteq R$, $Jq \subseteq R$ as well. Hence $RJq \subseteq R$. Letting I denote RJ, we note that $l_R(I) = 0$ and so $I \in \mathcal{I}(R)$ (see Proposition 2.1.1 and Remark 2.1.4). Further, again since $Iq, [R, q] \subseteq R$, $qI \subseteq R$ as well and so $q \in Q_s$.

Note that D_i is a Lie ideal of $Der(Q)$, and in fact we have the specific formula:

$$[ad(q), \delta] = ad(q^\delta). \tag{2.11}$$

The Lie ring in which we are primarily interested is

$$D = D(R) = Der(R)C + D_i.$$

If R is a prime ring and Φ is the prime subfield of C, then D is a Lie algebra over Φ.

We now turn our attention to the set of all automorphisms and antiautomorphisms of a semiprime ring R. This set forms a group under composition of mappings and we denote this group by $G = G(R)$.

Proposition 2.5.3 *Any automorphism σ of a semiprime ring R can be extended uniquely to an automorphism of Q_{mr} (we shall let σ also denote its extension to Q_{mr}). Furthermore $Q_r^\sigma = Q_r$ and $Q_s^\sigma = Q_s$.*

Proof. Let $q \in Q_{mr}$. Then $qJ \subseteq R$ for some dense right ideal J of R. Setting $I = J^\sigma$, we note that I is a dense right ideal of R. Define $f : I \to R$ by the rule $f(x) = (qx^{\sigma^{-1}})^\sigma$ for all $x \in I$. Then for $r \in R$ we have

$$f(xr) = (q(xr)^{\sigma^{-1}})^\sigma = ((qx^{\sigma^{-1}})r^{\sigma^{-1}})^\sigma = (qx^{\sigma^{-1}})^\sigma r = f(x)r$$

and so $[f;\, I] \in Q_{mr}$. We define $q^\sigma = [f;\, I]$. Clearly the mapping $\sigma : Q_{mr} \to Q_{mr}$ is additive, and so σ has been extended uniquely to an element σ of $End_{\mathbb{Z}}(Q_{mr})$ such that

$$q^\sigma x^\sigma = (qx)^\sigma \quad \text{for all} \quad x \in J. \tag{2.12}$$

Note that $q^\sigma J^\sigma \subseteq R$.

Let now $p, q \in Q_{mr}$. By Lemma 2.1.8 $qJ \subseteq (p : R)_R$ for some dense right ideal J of R. It follows from (2.12) that for $x \in J$ we have

$$(pq)^\sigma x^\sigma = (pqx)^\sigma = (p(qx))^\sigma = p^\sigma (qx)^\sigma = p^\sigma q^\sigma x^\sigma$$

and so $(pq)^\sigma = p^\sigma q^\sigma$. Therefore σ is an endomorphism of Q_{mr}. Applying the above argument to σ^{-1}, we conclude that σ is invertible and so an automorphism of Q_{mr}. Obviously $Q_r^\sigma = Q_r$ and $Q_s^\sigma = Q_s$.

Proposition 2.5.4 *Any antiautomorphism σ of a semiprime ring R can be extended uniquely to an antiautomorphism of $Q = Q_s$ (and thus we have $G(R) \subseteq G(Q)$).*

Proof. Let $q \in Q$. Then $qJ + Jq \subseteq R$ for some dense ideal J of R. Note that $I = J^\sigma$ is a dense ideal of R as well. We define $f : I \to R$ by the rule $f(x) = (x^{\sigma^{-1}} q)^\sigma$. It is easy to check that f is a homomorphism of right R-modules and so $\{f; I\} \in Q_r$. We set $q^\sigma = \{f; I\}$ and note that

$$q^\sigma x^\sigma = (xq)^\sigma \quad \text{for all} \quad x \in J.$$

Further, for all $a, b \in J$ we have

$$a^\sigma q^\sigma b^\sigma = a^\sigma (bq)^\sigma = (bqa)^\sigma = (qa)^\sigma b^\sigma$$

and so $(qa)^\sigma = a^\sigma q^\sigma$. It follows that $q^\sigma \in Q_s$ and hence $\sigma : Q_s \to Q_s$. Clearly σ is an additive mapping. Let now $p, q \in Q$. Choose a dense ideal J of R such that Jp, pJ, Jq, qJ, Jpq, pqJ are all contained in R and let $I = J^2$. Then $Iq, qI, Ip, pI \subseteq J$. For all $x \in I$ we have

$$(pq)^\sigma x^\sigma = (xpq)^\sigma = q^\sigma (xp)^\sigma = q^\sigma p^\sigma x^\sigma,$$

which implies that $(pq)^\sigma = q^\sigma p^\sigma$. Now it is clear that σ is an antiautomorphism of Q.

We let $G_i = G_i(R)$ be the set of all automorphisms σ of R for which there exists an invertible element $t \in Q_{mr}$ such that $r^\sigma = t^{-1}rt$ for all $r \in R$ (i.e., $\sigma = inn(t)$). It is easy to see that in fact $t \in Q_s$. Following S. Montgomery such automorphism is called X-*inner* and the element t is called a *normalizing element* for R. Clearly G_i is a normal subgroup of G and includes the ordinary inner automorphisms of R.

In Chapter 7 certain mappings involving derivations, automorphisms, and antiautomorphisms will be very useful in induction arguments, and we now describe some of them.

Consider the ring $Q^\circ \otimes_{\mathcal{Z}} Q$, the tensor product of $Q = Q_{mr}(R)$ and its opposite ring Q° over the integers $\mathcal{Z}$, and the ring $End_{\mathcal{Z}}(Q)$. For any $\epsilon \in End_{\mathcal{Z}}(Q)$ the mapping of $Q^\circ \otimes_{\mathcal{Z}} Q$ into $Q^\circ \otimes_{\mathcal{Z}} Q$ given by $a \otimes b \mapsto a^\epsilon \otimes b$ is always well-defined. Further for $\beta = \sum_j x_j \otimes y_j \in Q^\circ \otimes_{\mathcal{Z}} Q$ we denote the image under this map by β^ϵ. The mapping $x \mapsto \sum_j x_j x y_j$, $x \in Q$ is also well-defined and we denote the image under this mapping by $x \cdot \beta$. Clearly Q is a right $Q^\circ \otimes_{\mathcal{Z}} Q$-module under the multiplication $x \cdot \beta$, $x \in Q$, $\beta \in Q^\circ \otimes_{\mathcal{Z}} Q$.

We will often be interested in cutting down the domain of mappings to subsets $N_{I,J}$ of $Q^\circ \otimes_{\mathcal{Z}} Q$ defined as follows: given $I \in \mathcal{I}(R)$, $J \in \mathcal{D}(R)$, $N_{I,J}$ is the subring of $Q^\circ \otimes_{\mathcal{Z}} Q$ generated by all elements of the form $r \otimes r'$, where $r \in I$, $r' \in J$. In case $I = J \in \mathcal{I}(R)$ we let $N_I = N_{I,I}$. We remark that N_I is always an ideal of $N = N_R$ and $N_{I,J}$ is always a right ideal of N.

Remark 2.5.5 *Let R be a semiprime ring with extended centroid C, $Q = Q_{mr}(R)$, I a dense ideal of R and $q_1, q_2, \ldots, q_n \in Q$. Suppose that $q_1 \notin \sum_{i=2}^n Cq_i$. Then there exists $\beta \in N_I$ such that*

$$q_1 \cdot \beta \neq 0 \quad \textit{but} \quad q_i \cdot \beta = 0 \quad \textit{for all} \quad i = 2, 3, \ldots, n.$$

Proof. By Proposition 2.1.10, $Q_{mr}(I) = Q$. Now applying Theorem 2.3.3 (with I instead of R), we complete the proof.

Of particular interest to us is the situation where $\epsilon = \sigma$, an element of $G = G(R)$ (especially when $\sigma \in Aut(R)$), or $\epsilon = \delta$, an element of $D = D(R)$.

For $\sigma \in Aut(R)$ the map $\beta \mapsto \beta^\sigma$ is a ring homomorphism.

For $\delta \in D$ and $y \in Q$, and $\beta \in Q^\circ \otimes_Z Q$ we have the following formulas whose straightforward verification will be left to the reader.

$$\begin{array}{lll} \text{If} \quad \gamma = \beta(y \otimes 1), & \text{then} & \gamma^\delta = \beta^\delta(y \otimes 1) + \beta(y^\delta \otimes 1); \\ \text{If} \quad \gamma = \beta(1 \otimes y), & \text{then} & \gamma^\delta = \beta^\delta(1 \otimes y). \end{array} \tag{2.13}$$

Associated with each element $\sigma \in Aut(R)$ is the set

$$M_\sigma = \{s \in Q_{mr} \mid rs = sr^\sigma \quad \text{for all} \quad r \in R\}.$$

Clearly M_σ is a C-submodule of Q_{mr}. It is called the *conjugation module* of σ . If $\tau \in Aut(R)$, then one can easily prove that

$$M_\sigma M_\tau = M_{\sigma\tau}. \tag{2.14}$$

We next note that

$$M_\sigma \subseteq Q_s. \tag{2.15}$$

Indeed, let $0 \neq t \in M_\sigma$. We have $tI \subseteq R$ where $I = (t : R)_R$. Clearly $I^{\sigma^{-1}}t = tI \subseteq R$ and so for $J = RI^{\sigma^{-1}}$ we have $Jt \subseteq R$ and $J \in \mathcal{I}(R)$. Now from $Jt = tJ^\sigma$ we conclude that $t \in Q_s$.

Another characterization of M_σ for prime rings is given in the following

Lemma 2.5.6 *Let R be a prime ring, $\sigma \in Aut(R)$ and $Q = Q_s$. Then*

$$M_\sigma = \{s \in Q \mid s \textit{ is invertible in } Q \textit{ and } \sigma = inn(s)\} \cup \{0\}.$$

Proof. It is immediate that M_σ contains the right side of the above equation. Let $0 \neq s \in M_\sigma$. By (2.15) there exists a dense ideal K of R such that $Ks + sK \subseteq R$. We next note that sK is an ideal of R since $rsK = sr^\sigma K$ for all $r \in R$. The mapping $f : sK \to R$ given by $sk \mapsto k$ is well-defined since if $sk = 0$, then $0 = rsk = sr^\sigma k$ for all $r \in R$ which implies that $k = 0$. Clearly f is a right R-module map and thus determines an element $q \in Q_r$ such that $qsk = k$ for all $k \in K$. It follows that $qs = 1$, and from $sqsk = sk$ for all $sk \in sK$ we see that $sq = 1$ and so s is invertible in Q_r. From the definition of s we then have $s^{-1}rs = r^\sigma$ and $s^{-1}r = r^\sigma s^{-1}$ for all $r \in R$. Substituting $r = a^{\sigma^{-1}}$, we obtain $as^{-1} = s^{-1}a^{\sigma^{-1}}$ for all $a \in R$, i.e. $s^{-1} \in M_{\sigma^{-1}}$. Hence from (2.15) we infer that $s^{-1} \in Q$ and so s is invertible in Q. The proof is complete.

Corollary 2.5.7 *Let R be a prime ring and $\sigma \in Aut(R)$. Then $M_\sigma \neq 0$ if and only if $\sigma \in G_i$.*

Remark 2.5.8 *If $\sigma = 1$, then $M_\sigma = C$.*

Now we generalize the notion of C-independence as follows:

Let $q_1, q_2, \dots, q_n \in Q_{mr}$ and $\sigma_1, \sigma_2, \dots, \sigma_n \in Aut(R)$. Then q_1 is said to be *left dependent* on $q_2, q_3, \dots, q_n$ re $\sigma_1, \sigma_2, \dots, \sigma_n$ if $q_1 \in \sum_{i=2}^n M_{\sigma_1^{-1}\sigma_i} q_i$ (for $n = 1$ $q_1 = 0$).

Equivalently, q_1 is *left independent* of $q_2, \dots, q_n$ re $\sigma_1, \dots, \sigma_n$ if $q_1 \notin \sum_{i=2}^n M_{\sigma_1^{-1}\sigma_i} q_i$ with $q_1 \neq 0$ in case $n = 1$.

In view of the preceding remark, if each $\sigma_i = 1$, then the notion of left independence coincides with C-independence. We now prove a useful "weak density" result for left independence due to Kharchenko.

Theorem 2.5.9 *Let R be a semiprime ring, $Q = Q_{mr}(R)$, $I \in \mathcal{I}(R)$, $J \in \mathcal{D}(R)$ and let q_1 be left independent of $q_2, q_3, \dots, q_n$ re $\sigma_1, \sigma_2, \dots, \sigma_n$ where $q_i \in Q$, $\sigma_i \in Aut(R)$. Then there exists $\beta \in N_{I,J}$ such that $q_1 \cdot \beta^{\sigma_1} \neq 0$ and $q_i \cdot \beta^{\sigma_i} = 0$ for all $i \geq 2$.*

Proof. The proof is by induction on n. The result is clear for $n = 1$ since $I^{\sigma_1}q_1J \neq 0$. We now assume the result true for $n-1$ and prove it for n. We suppose it is not true for n. By Lemma 2.1.8 there exists $L \in \mathcal{D}(R)$ such that $L \subseteq J$ and $q_iL \subseteq R$ for all $i = 1, 2, \ldots, n$. We let $N' = N_{I,L}$ and set

$$B = \{\beta \in N' \mid q_i \cdot \beta^{\sigma_i} = 0 \quad \text{for} \quad i = 2, 3, \ldots, n-1\}$$

(in case $n = 2$, we just set $B = N'$). It is easy to see that B is a right ideal of the ring $R^{\circ} \otimes R$. Hence $K = \{q_n \cdot \beta^{\sigma_n} \mid \beta \in B\}$ (which lies in R since $q_nL \subseteq R$) is an ideal of R (since it is a subbimodule of the right $R^{\circ} \otimes R$-module R). Suppose that $K = 0$. Applying the induction assumption to $q_1, q_2, \ldots, q_{n-1}$, we find an element $\beta \in N'$ such that $q_1 \cdot \beta^{\sigma_1} \neq 0$ and $q_i \cdot \beta^{\sigma_i} = 0$ for all $i = 2, 3, \ldots, n-1$. Clearly $\beta \in B$. Hence $q_n \cdot \beta^{\sigma_n} = 0$ and our statement is proved. Therefore we may assume that $K \neq 0$. Now we define $f : K \to R$ by the rule $q_n \cdot \beta^{\sigma_n} \mapsto q_1 \cdot \beta^{\sigma_1}$, $\beta \in B$. By our assumption that the theorem is not true we see that f is well-defined. Clearly f is a right R-module homomorphism. By Proposition 2.2.2 there exists an element $t \in Q_r$ such that $f(x) = tx$ for all $x \in K$. This means that $t(q_n \cdot \beta^{\sigma_n}) = q_1 \cdot \beta^{\sigma_1}$ for all $\beta \in B$. Now let $\beta = \sum_j x_j \otimes y_j \in B$ and $r \in R$. Setting $\gamma = \beta(r \otimes 1)$, we note that $\gamma \in B$. We have

$$\begin{aligned} tr^{\sigma_n}(q_n \cdot \beta^{\sigma_n}) &= \sum_j tr^{\sigma_n}x_j^{\sigma_n}q_ny_j = \sum_j t(rx_j)^{\sigma_n}q_ny_j \\ &= t(q_n \cdot \gamma^{\sigma_n}) = q_1 \cdot \gamma^{\sigma_1} = \sum_j (rx_j)^{\sigma_1}q_1y_j \\ &= \sum_j r^{\sigma_1}x_j^{\sigma_1}q_1y_j = r^{\sigma_1}(q_1 \cdot \beta^{\sigma_1}) = r^{\sigma_1}t(q_n \cdot \beta^{\sigma_n}) \end{aligned}$$

and hence $(tr^{\sigma_n} - r^{\sigma_1}t)k = 0$ for all $k \in K$, i.e., $(tr^{\sigma_1^{-1}\sigma_n} - rt)K = 0$ for all $r \in R$. Setting $e = E(K)$ and $U = r_R(K)$, we recall from Theorem 2.3.9 that $eU = 0$. Therefore $(ter^{\sigma_1^{-1}\sigma_n} - rte)(K+U) = 0$, whence $ter^{\sigma_1^{-1}\sigma_n} - rte = 0$ since $K + U \in \mathcal{I}(R)$. It follows that $s = te \in M_{\sigma_1^{-1}\sigma_n}$. Since $ke = k$ for all $k \in K$, $sk = tk = f(k)$. Now $q_1 - sq_n$ must be left independent of $q_2, q_3, \ldots, q_{n-1}$ re $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ since otherwise $q_1 - sq_n \in \sum_{i=2}^{n-1} M_{\sigma_1^{-1}\sigma_i} q_i$, that is, $q_1 \in \sum_{i=2}^{n} M_{\sigma_1^{-1}\sigma_i} q_i$, a contradiction to the original hypothesis. By our induction hypothesis again, this time applied to $q_1 - sq_n, q_2, \ldots, q_{n-1}$ re $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ there exists $\beta \in B$ such that $(q_1 - sq_n) \cdot \beta^{\sigma_1} \neq 0$. But on the other hand, writing $\beta = \sum_j x_j \otimes y_j$, we have

$$(sq_n) \cdot \beta^{\sigma_1} = \sum x_j^{\sigma_1} sq_n y_j = \sum sx_j^{\sigma_n} q_n y_j = s(q_n \cdot \beta^{\sigma_n}) = q_1 \cdot \beta^{\sigma_1}$$

and thus we have the contradiction $(q_1 - sq_n) \cdot \beta^{\sigma_1} = 0$. The theorem is thereby proved.

This Page Intentionally Left Blank

Chapter 3

The Method of Orthogonal Completions

Our goal in this chapter is to describe the method of orthogonal completions (see [25], [33], [32], [35], and [228]). In the study of semiprime rings it turns out to be useful if one can reduce the problem to the case of prime rings. However, directly factoring a semiprime ring by a prime ideal turns out to be ineffective in certain cases. For example, it is known (special case of Theorem 6.4.4) that every polynomial identity of a prime ring R is an identity of its maximal right ring of quotients $Q_{mr}(R)$. It is natural to try to prove an analogous result for semiprime rings. The direct reduction to the case of prime rings is difficult here, since, in general, there is no homomorphism $Q_{mr}(R) \to Q_{mr}(R/P)$ for a prime ideal P of R.

Similar difficulties arise in considering a number of other questions connected with the maximal right ring of quotients of semiprime rings, in the study of semiprime rings with involution or in the study of derivations of semiprime rings. As we shall show, many of this difficulties of reducing the "semiprime case" to the "prime case" can be successfully overcome by the method of orthogonal completions.

3.1 Basic Notions and Constructions

In what follows C will be a von Neumann regular selfinjective commutative ring with 1. Clearly $Q_{mr}(C) = C$ and so

$$r_C(T) = (1 - E(T))C$$

for any subset $T \subseteq C$ by Theorem 2.3.9. A unital right C-module N is called *nonsingular* if for any element $0 \neq x \in N$ its right annihilator $r_C(x)$ is not essential.

Lemma 3.1.1 *Let N be a right C-module. Then the following conditions are equivalent:*

(i) N is nonsingular;

(ii) For any subset $T \subseteq N$ there exists a unique idempotent $E(T) \in C$ such that $r_C(T) = (1 - E(T))C$;

(iii) $E(Te) = E(T)e$ for any subset $T \subseteq N$ and $e = e^2 \in C$.

Proof. (i) $\Rightarrow$ (ii) Let $T \subseteq N$. Setting $e = E(r_C(T))$, we note that $I = (1 - e)C + r_C(T)$ is a dense ideal of C by Remark 2.1.5. Since $TeI = 0$, it follows from our assumptions that $Te = 0$ and so $e \in r_C(T)$. On the other hand $ec = c$ for all $c \in r_C(T)$ by Theorem 2.3.9**(i)**. Therefore $r_C(T) = eC$ and **(ii)** is proved. From **(ii)** it follows that $r_C(x) = (1 - E(x))C$ for all $x \in N$. Hence if $x \neq 0$, then $r_C(x)$ is not essential for and so N is nonsingular. The last statement is proved analogously to Theorem 2.3.9**(ii)**.

The criteria of Lemma 3.1.1 yields two corollaries. The first one follows directly from Theorem 2.3.9.

Corollary 3.1.2 *Let R be a semiprime ring. Then $Q_{mr}(R)$ is a nonsingular module over its center C.*

Corollary 3.1.3 *Let R be a semiprime ring, $Q = Q_{mr}(R)$ and $D = Der(Q)$. Then D is a nonsingular right C-module.*

Proof. Let $d \in D$. Then $r_C(d) = r_C(Q^d) = (1 - E(Q^d))C$ which completes the proof.

Applying the same arguments as in the proof of the Theorem 2.3.9(**iv**), one can prove the following

Remark 3.1.4 *Let N be a nonsingular right C-module, $M = \sum_{i=1}^{n} a_i C$ a finitely generated submodule of N and let k be the minimal number of generators of M. Then there exist elements $m_1, \dots, m_k \in M$ such that $M = \oplus_{i=1}^{k} m_i C$ and $E(m_i)E(m_{i+1}) = E(m_{i+1})$ for all $i = 1, \dots, k-1$.*

We set

$$B = B(C) = \{e \in C \mid e^2 = e\}.$$

A convenient partial ordering of B is given as follows: for $e, f \in B$ $e \leq f$ if $e = ef$. Clearly $e \leq f$ if and only if $1 - e \geq 1 - f$. A subset $U \subseteq B$ is called *dense* if $r_C(U) = 0$ (i.e., $E(U) = 1$). Further, a subset U is said to be *orthogonal* if $uv = 0$ for all $u \neq v \in U$. We note that for any dense orthogonal subsets $U, V \subseteq B$ the subset

$$UV = \{uv \mid u \in U,\ v \in V\} \tag{3.1}$$

is dense orthogonal as well.

Remark 3.1.5 *Let T be a subset of B such that $eT \subseteq T$ for any $e \in B$, and let V be a maximal orthogonal subset of T. Then $U = V \cup \{1 - E(T)\}$ is a dense orthogonal subset of B and $E(V) = E(T)$.*

Proof. Clearly U is an orthogonal subset of B. Suppose that $0 \neq e^2 = e \in r_C(U)$. Since $e(1 - E(T)) = 0$ and $r_C(T) = (1 - E(T))C$, we have $eT \neq 0$ and so $et \neq 0$ for some $t \in T$. By assumption $et \in T$. Then $V \cup \{et\}$ is an orthogonal subset of T. By the maximality of V we conclude that $et \in V$ and so $0 = (et)e = et$, a contradiction.

We set $e = E(V)$. Since $r_C(V) \supseteq r_C(T)$, we infer that $eE(T) = e$. Clearly $U(1-e)E(T) = 0$. By the density of U we conclude that $(1-e)E(T) = 0$ and so $E(T) = e$. The proof is complete.

In what follows N will be a nonsingular right C-module. A subset $T \subseteq N$ is called *orthogonally complete* if for any orthogonal dense subset $U \subseteq B$ and any subset $\{t_u \mid u \in U\} \subseteq T$ there exists an element $t \in T$ such that $tu = t_u u$ for all $u \in U$.

We note that the element $t \in T$ is uniquely determined by the conditions $tu = t_u u$ for all $u \in U$. Indeed, assume that for some $x \in N$ we have that $ux = ut_u$ for all $u \in U$. Then $(x-t)u = 0$ for all $u \in U$ and so $U \subseteq r_C(x-t) = (1-E(x-t))C$. Since U is dense, $r_C(x-t) = C$ and $x = t$. We denote this element t by

$$t = \sum_{u\in U}{}^{\perp} t_u u.$$

Now it is clear that the intersection of any family of orthogonally complete subsets of N is again orthogonally complete. Consider next an arbitrary orthogonal subset V of B and $t_v \in T$ where T is an orthogonally complete subset containing 0. Set $w = 1 - E(V)$, $U = V \cup \{w\}$ and $t_w = 0$. We then define $\sum_{v\in V}^{\perp} t_v v = \sum_{u\in U}^{\perp} t_u u$.

The following example plays a key role in the demonstration of connections of the orthogonally completion method with the classical Los and Horn theorems.

Example. Let $\{R_i \mid i \in I\}$ be a family of prime rings with extended centroids C_i and maximal right rings of quotients Q_i. It is easy to see that $Q = Q_{mr}\left(\prod_{i\in I} R_i\right) = \prod_{i\in I} Q_i$ and the extended centroid C of $\prod_{i\in I} R_i$ is equal to $\prod_{i\in I} C_i$. One can easily check that a subset $T \subseteq Q$ is orthogonally complete if and only if $T = \prod_{i=1} T_i$ where T_i is the canonical projection of T into Q_i.

The following proposition gives a characterization of orthogonally complete C-modules.

Proposition 3.1.6 *Let N be a nonsingular C-module. Then N is orthogonally complete if and only if N is an injective C-module.*

Proof. Suppose that N is orthogonally complete and let $f : L \to N$ is a homomorphism of an ideal L of the ring C. According to Baer's criteria, it is enough to prove that there exists an element $x \in N$ such that $f(y) = xy$ for all $y \in L$. Let V be a maximal orthogonal subset of $L \cap B$. Since C is von Neumann regular, $L = C(L \cap B)$ and so $E(L) = E(L \cap B)$. By Remark 3.1.5, $U = V \cup \{1 - E(L)\}$ is a dense orthogonal subset of $B = B(C)$. We set $x_v = f(v)$ for all $v \in V$, $w = 1 - E(V)$, $x_w = 0$ and $x = \sum_{u \in U}^{\perp} x_u u$. Let now $y \in L$. Then for all $v \in V$ we have

$$(xy)v = (xv)y = x_v vy = f(v)vy = f(vy) = f(yv) = f(y)v.$$

Since $Vw = 0$, $Lw = 0$ as well. Hence $yw = 0$ and

$$(xy)w = (xw)y = 0 = f(yw) = f(y)w.$$

Therefore $r_C(xy - f(y)) \supseteq U$ and so $r_C(xy - f(y)) = C$, and $f(y) = xy$. Hence N is injective.

Assume now that N is injective and let U be dense orthogonal subset of B, $x_u \in N$, $u \in U$. Note that $L = \sum_{u \in U} uC = \oplus_{u \in U} uC$. Define a homomorphism $f : L \to N$ by the rule $f(u) = x_u u$, $u \in U$, and its consequences. By assumption there exists an element $x \in N$ such that $f(y) = xy$ for all $y \in L$. In particular $xu = f(u) = x_u u$ for all $u \in U$ and so N is orthogonally complete.

We continue with the following useful remarks.

Remark 3.1.7 *Let R be a semiprime ring with extended centroid C, $U \subseteq B(C)$ a dense orthogonal subset, $I_u = (u : R)_R$, $D_u \in \mathcal{D}(R)$, $u \in U$. Then:*

(i) $I = \sum_{u \in U} I_u u$ is a dense ideal of R;

(ii) $D = \sum_{u \in U} D_u I_u u$ is a dense right ideal of R.

Proof. Since $u \in C$, I_u is a dense ideal of R. Hence I is an ideal of R. Consider $x \in r_R(I)$. We have $I_u ux = 0$ for all $u \in U$. As I_u is dense, $xu = ux = 0$ by Proposition 2.1.7. Hence $U \subseteq r_C(x) = (1 - E(x))C$ and so $r_C(x) = C$ by the density of U. It follows that $x = 0$ and so I is dense.

Now let $r_1, r_2 \in R$ with $r_1 \neq 0$. Hence $E(r_1) \neq 0$ and so $uE(r_1) \neq 0$ for some $u \in U$. By Theorem 2.3.9**(ii)** $E(ur_1) = uE(r_1) \neq 0$ and hence $ur_1 \neq 0$ as well. Since D_u is a dense right ideal of R, there exists an element $r' \in R$ such that $ur_1r' \neq 0$ and $r_2r' \in D_u$. Recalling that I_u is a dense ideal of R, we infer that $ur_1r'r'' \neq 0$ for some $r'' \in I_u$. Setting $r = ur'r''$, we note that $r_2r = r_2r'r''u \in D_uI_uu \subseteq D$ and $r_1r \neq 0$. Thus D is a dense right ideal of R.

Remark 3.1.8 *Let* $x = \sum_{u \in U}^{\perp} x_u u \in N$, $y = \sum_{v \in V}^{\perp} y_v v \in N$ *where* $x_u, y_v \in N$ *and* U, V *are dense orthogonal subsets of* B. *Then* $x + y = \sum_{uv \in UV}^{\perp}(x_u + y_v)uv$.

Proof. By (3.1) UV is a dense orthogonal subset of B. For all $u \in U$, $v \in V$ we have

$$(x + y)uv = (xu)v + (yv)u = x_u uv + y_v uv = (x_u + y_v)uv$$

which means that $x + y = \sum_{uv \in UV}^{\perp}(x_u + y_v)uv$.

The proof of the following remark is similar to that of the preceding one and is left to the reader.

Remark 3.1.9 *Let* R *be a semiprime ring with extended centroid* C, $Q = Q_{mr}(R)$, $a \in Q$, $x = \sum_{u \in U}^{\perp} x_u u \in Q$, $y = \sum_{v \in V}^{\perp} y_v v \in Q$ *where* $x_u, y_v \in Q$ *and* U, V *are dense orthogonal subsets of* $B(C)$. *Then* $xy = \sum_{uv \in UV}^{\perp} x_u y_v uv$ *and* $xa = \sum_{u \in U}^{\perp} x_u au$.

Now we are in a position to prove the following important results.

Proposition 3.1.10 *Let R be a semiprime ring, $Q_s = Q_s(R)$, $Q_r = Q_r(R)$, $Q_{mr} = Q_{mr}(R)$, and $D_i = \{ad(q) \mid q \in Q\}$. Then each of the right C-modules Q_{mr}, Q_r, Q_s and D_i is orthogonally complete.*

Proof. Let $\{q_u \mid u \in U\} \subseteq Q_{mr}$ where U is a dense orthogonal subset of B. We set $I_u = (u : R)_R$, $D_u = (q_u : R)_R$ and $D = \sum_{u\in U} D_u I_u u$. By Remark 3.1.7 D is a dense right ideal of R. Since U is an orthogonal subset, $D = \oplus_{u\in U} D_u I_u u$. Define a homomorphism of right R-modules $f : D \to R$ by the rule $f(d_u i_u u) = q_u d_u i_u u$ (where $d_u \in D_u$ and $i_u \in I_u$) and its consequences. Setting $q = [f; D] \in Q_{mr}$, we note that $q d_u i_u u = q_u d_u i_u u$ and so $(qu - q_u u) d_u i_u = 0$ for all $d_u \in D_u$ and $i_u \in I_u$. Since I_u and D_u are dense right ideals, we have $qu = q_u u$ for all $u \in U$ and so Q_{mr} is orthogonally complete.

If in the above consideration all q_u are in Q_r, then we take each D_u to be some dense ideal of R such that $q_u D_u \subseteq R$. Hence D is a dense ideal of R and so $q \in Q_r$. If all q_u are in Q_s, we can assume that the dense ideals D_u are chosen in such a way that $q_u D_u + D_u q_u \subseteq R$. Then one can easily check that $Dq \subseteq R$ which implies that $q \in Q_s$.

Now let be given $U \subseteq B$ a dense orthogonal subset. For any subset $\{ad(q_u) \mid q_u \in Q_s\} \subseteq D_i(R)$ we set $q = \sum^{\perp}_{u\in U} q_u u$ and note that $(xq - qx)u = x(qu) - (qu)x = (xq_u - q_u x)u$ for all $x \in Q$ and $u \in U$. Hence $ad(q)u = ad(q_u)u$ for all $u \in U$ which completes the proof.

Proposition 3.1.11 *Let $0 \in T$ be an orthogonally complete subset of a nonsingular right C-module N. Then:*

(i) $Te \subseteq T$ for all $e \in B(C)$;

(ii) There exists an element $t \in T$ such that $E(t) = E(T)$ (or, equivalently, $r_C(T) = r_C(t)$).

Proof. (i) Let $x \in T$ and $e \in B$. Since T is orthogonally complete, there exists an element $y \in T$ such that $ye = xe$ and $y(1 - e) = 0$. It follows that $y = ye = xe$ and so $xe \in T$.

(ii) Consider the set $W = \{E(x) \mid x \in T\}$. By Lemma 3.1.1 **(iii)** we have $E(xe) = E(x)e$ for all $e \in B$ and $x \in T$. Hence $We \subseteq W$. Let V be a maximal orthogonal subset of W and $U = V \cup \{1 - E(W)\}$. According to Remark 3.1.5 U is a dense orthogonal subset of B. By definition of the set W for every $v \in V$ there exists an element $t_v \in T$ such that $v = E(t_v)$. Set $t_{1-E(W)} = 0$ and $t = \sum_{u\in U}^{\perp} t_u u$. Clearly $t \in T$. We claim that $E(t) = E(T)$. It is enough to prove that $r_C(T) = r_C(t)$. Clearly $r_C(t) \supseteq r_C(T)$. Suppose $r_C(t) \neq r_C(T)$. Then $(1 - E(t))x \neq 0$ for some $x \in T$. We set $e = 1 - E(t)$, $y = ex$ and $w = E(y)$. Note that $w \neq 0$ since $y \neq 0$. From Lemma 3.1.1**(iii)** we infer that $w = ew$. Since $te = 0$, we have $0 = t(vw) = (tv)w = t_v vw$ for all $v \in V$. Therefore $vw \in r_C(t_v) = (1 - v)C$ and so $vw = 0$ for all $v \in V$, a contradiction to the maximality of V. Thus $E(t) = E(T)$.

Proposition 3.1.12 *Let R be a semiprime ring $Q = Q_{mr}(R)$ and $\sigma \in Aut(R)$. Then M_σ is a cyclic C-module and its generator m_σ is an invertible element of the ring $QE(m_\sigma)$.*

Proof. We claim that M_σ is an orthogonally complete subset of Q. Indeed, let U be a dense orthogonal subset of $B = B(C)$ and $m_u \in M_\sigma$, $u \in U$. Consider the element $m = \sum_{u\in U}^{\perp} m_u u$. According to Remark 3.1.9 we have

$$xm = \sum_{u\in U}^{\perp} xm_u u = \sum_{u\in U}^{\perp} m_u x^\sigma u = mx^\sigma$$

for all $x \in R$. Therefore $m \in M_\sigma$ and our claim is proved.

By Proposition 3.1.11 $E(M_\sigma) = E(m)$ for some $m \in M_\sigma$. Let $e = E(m)$, $I = (e : R)_R$, $J = eI$ and $K = r_R(J)$. Clearly $J \oplus K$ is a dense ideal of R. We note that $mJ = J^{\sigma^{-1}} m$ is an ideal of R and $mJK = 0$. We claim that $r_R(mJ) = K$. If $mJr = 0$ where $r \in R$, then $meIr = mJr = 0$. Since I is a dense ideal of R,

$Q_{mr}(I) = Q$ by Proposition 2.1.10. It follows from Lemma 2.3.10 that $E(me)r = 0$. Recall that $e = E(m)$ and $me = m$. Hence $er = 0$ and $Jr = Ier = 0$ which proves our claim. Define a homomorphism of right R-modules $f : mJ \oplus K \to J \oplus K$ by the rule $mx + y \mapsto x$ for all $x \in J$, $y \in K$. If $mx = 0$ where $x \in J$, then $mJx = J^{\sigma^{-1}}mx = 0$ and so $x \in J \cap K = 0$. Therefore f is well-defined. Setting $q = [f; mJ + K] \in Q$, we note that $qe = q$ and $qm = e$. Note that $IeK = JK = 0$. Since I is dense, $eK = 0$. Hence $mqK = (me)qK = mqeK = 0$. It follows that $(mq - e)(mJ + K) = 0$ and so $mq = e$. Therefore m is an invertible element of the ring eQ. Clearly $rq = qr^{\sigma^{-1}}$ for all $r \in R$. Hence $rm'q = m'qr$ for all $r \in R$, $m' \in M_\sigma$. It follows that $M_\sigma q \subseteq C$ and so $M_\sigma = M_\sigma e = M_\sigma qm \subseteq Cm$. The proof is complete.

We set $i(\sigma) = E(M_\sigma)$. It follows from the above result that the ring $Q = Q_{mr}(R)$ is a direct sum $Q = Qi(\sigma) \oplus Q(1 - i(\sigma))$ of σ-invariant ideals and σ induces an inner automorphism on $Qi(\sigma)$.

Now let μ be a derivation of a semiprime ring R and $Q = Q_{mr}(R)$. We set

$$M_\mu = \{m \in Q \mid rm - mr = E(m)r^\mu \quad \text{for all} \quad r \in R\}.$$

Since $E(ex) = eE(x)$ for all $e \in B(C)$ and $x \in Q$, we conclude that $M_\mu e \subseteq M_\mu$. We leave for the reader the straightforward verification of the following remark (see the proof of (2.15) in section 2.5).

Remark 3.1.13 *The subset M_μ is orthogonally complete and $M_\mu \subseteq Q_s$.*

We set $i(\mu) = E(M_\mu)$ and note that $i(\mu) = E(m)$ for some $m \in M_\mu$ according to Proposition 3.1.11. Clearly μ induces the inner derivation $ad(m)$ on the direct summand $Qi(\mu)$.

Let N be an orthogonally complete nonsingular C-module and $T \subseteq N$ a subset. The intersection of all orthogonally complete subsets of N containing T is called *the orthogonal completion* of T and is denoted by $O(T)$.

Since the intersection of orthogonally complete subsets is orthogonally complete, $O(T)$ is an orthogonally complete subset as well.

Proposition 3.1.14 *Let N be a nonsingular orthogonally complete right C-module and $T \subseteq N$ a subset. Then*

$$O(T) = \quad \{\sum_{u\in U}{}^{\perp} t_u u \mid U \quad \textit{is a dense orthogonal subset} \\ \textit{of} \quad B \quad \textit{and} \quad \{t_u \mid u \in U\} \subseteq T\}.$$

Proof. Letting H denote the right side of the above equality, we note that it is enough to prove that H is orthogonally complete. To this end consider any dense orthogonal subset W of B and let $h_w = \sum^{\perp}_{u_w \in U_w} x_{u_w} u_w \in H$, $w \in W$, where $x_{u_w} \in T$ and U_w is a dense orthogonal subset of B. We set $V = \{wu_w \mid w \in W,\ u_w \in U_w\}$. One can easily check that V is a dense orthogonal subset of B. For $v = wu_w \in V$ we set $t_v = x_{u_w}$. We now claim that

$$\sum_{w\in W}{}^{\perp} h_w w = \sum_{v\in V}{}^{\perp} t_v v.$$

Indeed, for any $v = wu_w \in V$ we have

$$\left(\sum_{w\in W}{}^{\perp} h_w w\right) wu_w = h_w wu_w = (h_w u_w)w = x_{u_w} u_w w = t_v v$$

which completes the proof.

The following result follows directly from the preceding proposition, Proposition 3.1.10, Remark 3.1.8 and Remark 3.1.9.

Corollary 3.1.15 *Let R be a semiprime ring. Then:*

(i) its orthogonal completion $O(R)$ is a subring of the ring $Q_s(R)$;

(ii) If I is a (right) ideal of R, then $O(I)$ is a (right) ideal of $O(R)$ as well.

Example. We keep the notations of the preceding example. Let $R = \oplus_{i\in I} R_i \subseteq \prod_{i\in I} R_i$. Clearly $Q_{mr}(R) = \prod_{i\in I} Q_i$. It is easy to see that $O(R) = \prod_{i\in I} R_i$.

Remark 3.1.16 *Let R be a semiprime ring, $Q = Q_{mr}(R)$, $\mu \in Der(Q)$, $g \in G(Q)$ and $q = \sum^{\perp}_{u\in U} q_u u$ where $q_u \in Q$, $u \in U$. Then:*

$$q^\mu = \sum_{u\in U}{}^{\perp} q_u^\mu u \quad \textit{and} \quad q^g = \sum_{u\in U}{}^{\perp} q_u^g u^g.$$

Proof. We first note that

$$e^\mu = (e^2)^\mu = ee^\mu + e^\mu e = 2ee^\mu,\ e \in B.$$

Multiplying both sides by e, we infer that $ee^\mu = 2ee^\mu$ and so $ee^\mu = 0$. Hence $e^\mu = 2ee^\mu = 0$. We now have

$$q^\mu u = (qu)^\mu = (q_u u)^\mu = q_u^\mu u$$

for all $u \in U$ which implies the first formula. The second one is proved similarly.

Corollary 3.1.17 *Let R be a semiprime ring, $Q = Q_{mr}(R)$, $\mu \in Der(Q)$ and $g \in G(Q)$. Suppose that $R^\mu \subseteq R$ and $R^g = R$. Then $O(R)^\mu \subseteq O(R)$ and $O(R)^g = O(R)$ as well.*

We continue our discussion of orthogonally complete subsets with the following useful lemmas.

Lemma 3.1.18 *Let N be a nonsingular right C-module, $T_i \subseteq N$ an orthogonally complete subset of N containing 0, $1 \leq i \leq n$, and $f : T_1 \times T_2 \times \ldots T_n \to N$ a mapping such that $f(t_1, \ldots, t_n)e = f(t_1 e, \ldots, t_n e)$ for all $e \in B = B(C)$ and $t_i \in T_i$. Then $H = f(T_1, T_2, \ldots, T_n)$ is orthogonally complete.*

Proof. Let $U \subseteq B$ be a dense orthogonal subset and $h_u = f(t_{u1}, t_{u2}, \ldots, t_{un}) \in H$ for all $u \in U$ where $t_{ui} \in T_i$. Setting $t_i = \sum_{u\in U}^{\perp} t_{iu} u$, we leave to the reader the straightforward verification of the equality $\sum_{u\in U}^{\perp} h_u u = f(t_1, t_2, \ldots, t_n)$, which completes the proof.

The proof of the following lemma is straightforward and we leave it to the reader.

Lemma 3.1.19 *Let R be a semiprime ring and let T and H be orthogonally complete subsets of $Q = Q_{mr}(R)$. Then for any $a \in Q$ the subset*

$$(a : T)_H = \{h \in H \mid ah \in T\}$$

is either empty or orthogonally complete.

Theorem 3.1.20 *Let T be an orthogonally complete subset of $Q = Q_{mr}(R)$ containing 0, and let $q \in Q$. Then there exists a unique element $E(T;\, q) \in B = B(C)$ such that $q(1 - E(T;\, q)) \in T$ and $1 - E(T;\, q) \geq e$ for all $e \in B$ such that $qe \in T$. Further, $E(T;\, eq) = eE(T;\, q)$ for all $e \in B$.*

Proof. Since B is an orthogonally complete subset of Q, $L = (q : T)_B$ is orthogonally complete by Lemma 3.1.19. Because $0 \in T$ (and hence $0 \in L$) we have by Proposition 3.1.11 that $Te \subseteq T$ for all $e \in B$ and $E(L) = E(e_0) = e_0$ for some $e_0 \in L$. Clearly **(i)** $qe_0 \in T$ and **(ii)** $e \leq e_0$ for all $e \in L$ (since $ee_0 = eE(L) = e$). We see that $E(T;\, q) = 1 - e_0$ is the required element. Next let $e \in B$ and write $E(T; qe) = 1 - f_0$. We wish to prove that $1 - f_0 = e(1 - e_0)$. Indeed, from

$$qe(1 - e(1 - e_0)) = qee_0 \in Te \subseteq T$$

we have $1 - e(1 - e_0) \leq f_0$ and hence $e(1 - e_0) \geq 1 - f_0$ and so $e(1 - e_0) \geq e(1 - f_0)$. From $qef_0 \in T$ we have $ef_0 \leq e_0$ whence $1 - ef_0 \geq 1 - e_0$ and $e(1 - f_0) \geq e(1 - e_0)$. It follows that $e(1-e_0) = e(1-f_0) \leq 1-f_0 \leq e(1-e_0)$ and so $e(1-e_0) = 1-f_0$ and the theorem is proved.

We close this section with the following useful lemma.

Lemma 3.1.21 *Let $B = B(C)$ and $V = \{v_i \mid i \in I\}$ a subset of B such that $V \not\subseteq M$ for every $M \in Spec(B)$. Then there exists a finite subset $i_1, i_2, \ldots, i_k \in I$ and pairwise orthogonal idempotents $e_1, e_2, \ldots, e_k \in B$ whose sum is equal to* 1 *such that $e_j \leq v_{i_j}$ for all $j = 1, 2, \ldots, k$.*

Proof. We have that the ideal of the Boolean ring B generated by V is equal to B and so $1 = v_{i_1}b_1 \oplus \ldots \oplus v_{i_k}b_k$ for some $i_1, \ldots, i_k \in I$ and $b_j \in B$, where $\oplus$ is the Boolean addition (i.e., $u \oplus v = u + v - 2uv$ for all $u, v \in B$). Therefore $v_{i_1}B + v_{i_2}B + \ldots + v_{i_k}B = B$. We set $e_1 = v_{i_1}$. Suppose that we already have found pairwise orthogonal idempotents $e_1, e_2, \ldots, e_l$ such that $e_j \leq v_{i_j}$ and

$$\sum_{j=1}^{l} e_jB + \sum_{t=l+1}^{k} v_{i_t}B = B.$$

Then we set

$$e_{l+1} = v_{i_{l+1}}(1 - e_1 - e_2 - \ldots - e_l).$$

Continuing in this fashion we find pairwise orthogonal idempotents $e_1, e_2, \ldots, e_k$ such that $e_1 + \ldots + e_k = 1$ and $e_j \leq v_{i_j}$ for all j.

3.2 Pierce Stalks

The content of the present section will depend heavily on section 1.5.

Let R be a semiprime ring with extended centroid C, $B = B(C)$ and $Q = Q_{mr}(R)$. The ring R is called *orthogonally complete* , if $R = O(R)$. If R is orthogonally complete, then $eR \subseteq R$ for all $e \in B$ by Proposition 3.1.11. Let α be an ordinal number, $\tau : W(\alpha) \to \mathcal{N}$ and $\Omega = (\tau;\, \alpha)$. An Ω-ring R is said to be *orthogonally complete* if R is an orthogonally complete semiprime ring and for any $e \in B$, $\gamma \in W(\alpha)$ and $r_1, r_2, \ldots, r_n \in R$, where $n = \tau(\gamma)$, we have

$$eF_\gamma(r_1, r_2, \ldots, r_n) = F_\gamma(er_1, er_2, \ldots, er_n).$$

In what follows R will be an orthogonally complete Ω-ring with extended centroid C and $B = B(C)$. Given any term $t = t(x_1, x_2, \ldots, x_n)$ of signature Ω, $r_1, r_2, \ldots, r_n \in R$ and $e \in B$, one can easily prove by induction on a number of operation symbols appearing in t that

$$et(r_1, r_2, \ldots, r_n) = t(er_1, er_2, \ldots, er_n). \tag{3.2}$$

Let Δ_P be the set of all predicates either of type "$\|x \in T\|$", where T is an orthogonally complete subset of R containing 0, or "$\|x = y\|$". In what follows we will consider R as an Ω-Δ-ring.

It follows directly from the above definition that eR is an Ω-subring of R for all $e \in B$. Further, any predicate $\|x \in T\|$ where T is an orthogonally complete subset of R containing 0 defines a predicate on eR as on a subset of R. Here we note that if $x \in eR$, then $\|x \in T\| = 1$ if and only if $\|x \in eT\| = 1$.

Proposition 3.2.1 *Let R be an orthogonally complete Ω-Δ-ring, U an orthogonal subset of B and $e = \sum^{\perp}_{u\in U} u$. Then the mapping $\eta_U : \prod_{u\in U} Ru \to Re$ given by the rule $\{r_u u \mid u \in U\} \mapsto \sum^{\perp}_{u\in U} r_u u$ is an isomorphism of Ω-Δ-rings.*

Proof. Using the same argument as in the proofs of Remark 3.1.8 and Remark 3.1.9, one can easily prove that η_U is a homomorphism of Ω-rings. Clearly it is a monomorphism. Since

$$ea = \left(\sum_{u\in U}{}^{\perp} u\right) a = \sum_{u\in U}{}^{\perp} au,$$

η_U is surjective and so η_U is an isomorphism of Ω-rings. Now let T be an orthogonally complete subset of Re containing 0 and $x \in Re$. Since T is orthogonally complete and $e = \sum_{u\in U}^{\perp} u$, the inclusion $x \in T$ is equivalent to the inclusions $xu \in Tu$ for all $u \in U$. Therefore $\|x \in T\| = 1$ if and only if $\|xu \in Tu\| = 1$ for all $u \in U$. Recalling the definition of the Cartesian product of Ω-Δ-rings, we conclude that η_U is an isomorphism of Ω-Δ-rings.

Recall that B is a Boolean ring with addition given by the rule $u \oplus v = u + v - 2uv$ for all $u, v \in B$ and multiplication the same as that in C. We let $Spec(B)$ denote the set of all maximal ideals of the Boolean ring B. It is well known that an ideal M of B is maximal if and only if for any $e \in B$ either $e \in M$, or $1 - e = 1 \oplus e \in M$, but not both.

Let $M \in Spec(B)$. We set

$$RM = \{\sum_i r_i e_i \mid r_i \in R \quad \text{and} \quad e_i \in M\}.$$

Remark 3.2.2 *Let M be a maximal ideal of B and $a \in R$. Then:*

(i) $RM = \{x \in R \mid r_C(x) \cap (B \setminus M) \neq \emptyset\}$;

(ii) $a \in RM$ if and only if $E(a) \in M$.

Proof. (i) Let $x = \sum_{i=1}^{n} r_i e_i \in RM$ where $r_i \in R$, $e_i \in M$. We set $e = (1 - e_1)(1 - e_2)\dots(1 - e_n)$. Since $1 - e_i \notin M$, we see that $e \notin M$. Clearly $ex = 0$. On the other hand, let $ru = 0$ for some $u \in B \setminus M$. As $u \notin M$, $1 - u \in M$. Now we have $r = r(1 - u) \in RM$.

(ii) If $E(a) \in M$, then $a = aE(a) \in RM$. Conversely, let $a \in RM$. Then $ae = 0$ for some $e \in B \setminus M$. Since $e \in r_C(a) = (1 - E(a))C$, we infer that $1 - E(a) \notin M$. But then $E(a) = 1 - (1 - E(a)) \in M$.

Corollary 3.2.3 *Let $M \in Spec(B)$. Then RM is an ideal of the Ω-ring R.*

Proof. Being a sum of ideals Re, $e \in M$, RM is an ideal of the ring R. Let $\gamma \in W(\alpha)$, $n = \tau(\gamma)$, $r_1, r_2, \ldots, r_n \in R$ and $a_1, a_2, \ldots, a_n \in RM$. By Remark 3.2.2 for every index i there exists an idempotent $e_i \in B \setminus M$ such that $a_i e_i = 0$. Setting $s_i = r_i + a_i$ and $e = e_1 e_2 \ldots e_n$, we note that $s_i e = r_i e$ for all i. Therefore for $z = F_\gamma(s_1, \ldots, s_n) - F_\gamma(r_1, \ldots, r_n)$ we have

$$\begin{aligned} ez &= F_\gamma(es_1, \ldots, es_n) - F_\gamma(er_1, \ldots, er_n) \\ &= F_\gamma(er_1, \ldots, er_n) - F_\gamma(er_1, \ldots, er_n) = 0 \end{aligned}$$

and so $z \in RM$. Thus RM is an ideal of the Ω-ring R.

The factor Ω-ring R/RM is called the *Pierce stalk* of R at the point M of $Spec(B)$. Letting R_M denote the factor Ω-ring R/RM and $\phi_M : R \to R_M$ the canonical projection and taking into account Proposition 3.1.11 we summarize what has been proved in the following

Corollary 3.2.4 *Let R be an orthogonally complete Ω-ring, T an orthogonally complete subset of R containing 0 and $M \in Spec(B)$. Then:*

(i) *the canonical homomorphism $\phi_M : R \to R_M = R/RM$ of rings is a homomorphism of Ω-rings as well;*

(ii) $\ker(\phi_M) = \{r \in R \mid E(r) \in M\}$*;*

(iii) *$\phi_M(T) = 0$ if and only if $E(T) \in M$.*

Example With reference to the example of the preceding section, we consider $R = \prod_{i \in I} R_i$ and note that the extended centroid C of R coincides with $\prod_{i \in I} C_i$. Hence the Boolean ring $B = B(C)$ coincides with the set of all functions $I \to \mathcal{Z}_2$. Given any maximal ideal M of B, the set

$$\mathcal{T}_M = \{f^{-1}(0) \mid f \in B \setminus M\}$$

is an ultrafilter on I. We close this example with the note that $R_M = \prod_{i \in I} R_i / \mathcal{T}_M$.

We continue our discussion of properties of Pierce stalks with following lemmas.

Lemma 3.2.5 *Let R be an orthogonally complete Ω-ring, $a \in R$, T an orthogonally complete subset of R containing 0 and $M \in Spec(B)$. Then the following conditions are equivalent:*

(i) $\phi_M(a) \in \phi_M(T)$;

(ii) $ae \in T$ *for some* $e \in B \setminus M$;

(iii) $E(T;\, a) \in M$.

Proof. First of all we recall that $Te \subseteq T$ for all $e \in B$ by Proposition 3.1.11.

(i) ⇒ (ii) Let $\phi_M(a) \in \phi_M(T)$. Then $\phi_M(a) = \phi_M(t)$ for some $t \in T$. Hence $\phi_M(a - t) = 0$ and so $(a - t)e = 0$ for some $e \in B \setminus M$. Therefore $ae = te \in T$.

(ii) ⇒ (iii) Assume that $ae \in T$ for some $e \in B \setminus M$. By Theorem 3.1.20 we have that $e(1 - E(T;\, a)) = e$ and so $1 - E(T;\, a) \notin M$. Therefore $E(T;\, a) \in M$ by the maximality of M.

(iii) ⇒ (i) Let $u = E(T;\, a) \in M$. Then $a(1 - u) \in T$ and $au \in RM$. Thus $\phi_M(a) = \phi_M(a(1 - u)) \in \phi_M(T)$.

Lemma 3.2.6 *Let R be an orthogonally complete Ω-ring, $a \in R$, T and H orthogonally complete subsets of R containing 0 and $M \in Spec(B)$. Then:*

$$\phi_M((a : T)_H) = (\phi_M(a) : \phi_M(T))_{\phi_M(H)}.$$

Proof. Clearly $\phi_M((a : T)_H) \subseteq (\phi_M(a) : \phi_M(T))_{\phi_M(H)}$. Let $\phi_M(a)\phi_M(h) \in \phi_M(T)$ where $h \in H$. Then $ahe = te$ for some $e \in B \setminus M$ and $t \in T$. Clearly $he \in H$ and $te \in T$. Hence $he \in (a : T)_H$. Since $e \notin M$, $1 - e \in M$ and so $\phi_M(e) = 1$. Thus $\phi_M(h) = \phi_M(he) \in \phi_M((a : T)_H)$.

Now we are in a position to prove the following important result.

Theorem 3.2.7 *Let R be a semiprime orthogonally complete ring with extended centroid C, $B = B(C)$ and $M \in Spec(B)$. Then the ring $R_M = R/RM$ is prime.*

Proof. Suppose that $\phi_M(a)R_M\phi_M(b) = 0$ for some $a, b \in R$. Then $\phi_M(aRb) = 0$. Applying Lemma 3.1.18 to the mapping $R \to R$, $x \mapsto axb$, we conclude that aRb is an orthogonally complete subset of R. By Corollary 3.2.4 we have $e = 1 - E(aRb) \notin M$. Without loss of generality we can assume that $\phi_M(a) \neq 0$. Then $E(a) \notin M$. Now we have $e(aRb) = 0$. Hence according to Theorem 2.3.9(**ii**) and Lemma 2.3.10, $eE(a)b = E(ea)b = 0$. Since $eE(a) \notin M$, we conclude that $b \in \ker(\phi_M)$. Thus R_M is prime.

Let $\Phi(x_1, x_2, \ldots, x_n)$ be a first order formula of signature Ω-Δ, $\vec{a} = (a_1, a_2, \ldots, a_n) \in R^{(n)}$ and $v \in B$. We set $B^* = B \setminus \{0\}$, $v\vec{a} = (va_1, va_2, \ldots, va_n)$,

$$H(\Phi;\, \vec{a}) = \{e \in B^* \mid vR \models \Phi(v\vec{a}) \text{ for all } \quad 0 \neq v \leq e\} \cup \{0\}$$

and

$$E(\Phi(\vec{a})) = E(H(\Phi;\, \vec{a})).$$

In the case of the atomic formulas $\|x = y\|$ $x, y \in X$, and $\|x \in T\|$, T orthogonally complete with 0, the above concept takes a very concrete form. Indeed, we see that

$$H(\|x = y\|;\, a, b) = r_C(a - b) \cap B \tag{3.3}$$

since

$$\{e \in B^* \; |v(a-b) = 0 \text{ for all } 0 \neq v \leq e\} \cup \{0\} = r_C(a-b) \cap B.$$

From (3.3) it is immediate that

$$E(\|a = b\|) = 1 - E(a - b) \tag{3.4}$$

Similarly, we see that

$$H(\|x \in T\|, a) = (a : T)_B \tag{3.5}$$

since

$$\{e \in B^* \mid va \in T \text{ for all } 0 \neq v \leq e\} \cup \{0\} = (a : T)_B.$$

From (3.5) it is clear that

$$E(\|a \in T\|) = 1 - E(T;\, a) \tag{3.6}$$

in view of Theorem 3.1.20.

We have in fact proved parts **(i)** and **(iii)** of the following corollary, which will in turn provide the basis for induction in our main theorem.

Corollary 3.2.8 *Let R be an orthogonally complete Ω-ring, a, $b \in R$, T an orthogonally complete subset of R containing* 0 *and $M \in Spec(B)$. Then:*

(i) $E(\|a = b\|) = 1 - E(a - b)$;

(ii) $\|\phi_M(a) = \phi_M(b)\| = 1$ *if and only if* $E(\|a = b\|) \notin M$;

(iii) $E(\|a \in T\|) = 1 - E(T;\, a)$;

(iv) $\|\phi_M(a) \in \phi_M(T)\| = 1$ *if and only if* $E(\|a \in T\|) \notin M$.

Proof. **(ii)** follows from part **(i)** and Corollary 3.2.4(**ii**).
(iv) follows from part **(iii)** and Lemma 3.2.5(**iii**).

The following lemma plays an important role in the proof of Theorem 3.2.10, and it is here that Horn's Theorem (Theorem 1.5.5) is deployed.

Lemma 3.2.9 *Let R be an orthogonally complete Ω-Δ-ring, $\Phi(x_1, x_2, \ldots, x_n)$ a Horn formula of signature Ω-Δ in free variables $x_1, x_2, \ldots, x_n$, and $\vec{a} = (a_1, a_2, \ldots, a_n) \in R^{(n)}$. Then*

$$E(\Phi(\vec{a})) \in H(\Phi;\, \vec{a})$$

(i.e., $vR \models \Phi(v\vec{a})$ for all $0 \neq v \leq E(\Phi(\vec{a}))$).

Proof. We set $U = H(\Phi;\, \vec{a})$. It follows immediately from the definition that $eU \subseteq U$ for all $e \in B$. Let V be a maximal orthogonal subset of U. By Remark 3.1.5 we have $E(V) = E(U)$. Setting $w = \sum_{v\in V}^{\perp} v$, we note that $r_C(V) = (1-w)C$ and so $E(U) = E(V) = w$. If $w = 0$, then $w = 0 \in U$ and there is nothing to prove. Assume that $w \neq 0$ and let $0 \neq f \in wB$. We claim that $fR \models \Phi(f\vec{a})$. Indeed, let $V_0 = \{v \in V \mid vf \neq 0\}$. Note that

$$f = fw = \sum_{v\in V}{}^{\perp} fv = \sum_{v\in V_0}{}^{\perp} fv.$$

Since $V \subseteq H(\Phi;\, \vec{a})$, we have

$$Rvf \models \Phi(vf\vec{a}) \quad \text{for all} \quad v \in V_0.$$

By Theorem 1.5.5 it follows that

$$\left(\prod_{v\in V_0} Rvf\right) \models \Phi(\{fva_1\}_{v\in V_0}, \ldots, \{fva_n\}_{v\in V_0}).$$

According to Proposition 3.2.1, the mapping η given by the rule

$$\{fva\}_{v\in V_0} \mapsto \sum_{v\in V_0}{}^{\perp} afv = \left(\sum_{v\in V}{}^{\perp} v\right) fa = wfa = fa$$

is an isomorphism of Ω-Δ-rings $\prod_{v\in V_0} Rvf$ and $Rwf = Rf$. Hence $Rf \models \Phi(f\vec{a})$ for all $0 \neq f \in wB$ and so

$$E(\Phi(\vec{a})) = E(U) = w \in H(\Phi;\, \vec{a}).$$

We note that for $u, v \in B$ the inequality $u \leq v$ is equivalent to the statement that for all $M \in Spec(B)$ u not an element of M implies v not an element of M. We are now in a position to prove the main result of this chapter.

Theorem 3.2.10 *Let R be an orthogonally complete Ω-Δ-ring with extended centroid C, $B = B(C)$, $M \in Spec(B)$ and $\phi_M : R \to R_M = R/RM$ the canonical projection of Ω-Δ-rings. Further let $\Psi(x_1, x_2, \ldots, x_n)$ be a Horn formula of signature Ω-Δ and $\vec{a} = (a_1, a_2, \ldots, a_n) \in R^{(n)}$. Suppose that*

$$R_M \models \Psi(\phi_M(a_1), \ldots, \phi_M(a_n)).$$

Then $e = E(\Psi(\vec{a})) \notin M$ and $vR \models \Psi(v\vec{a})$ for all $0 \neq v \leq e$.

Proof. We set $\phi_M(\vec{a}) = (\phi_M(a_1), \phi_M(a_2), \ldots, \phi_M(a_n))$. First we suppose that Ψ is an atomic formula (i.e., a formula either of the type $\|t_1(x_1, x_2, \ldots, x_n) = t_2(x_1, x_2, \ldots, x_n\|$, where t_1, t_2 are terms, or of the type $\|x \in T\|$, where T is an orthogonally complete subset of R containing 0). Then it follows from Corollary 3.2.8 that $R_M \models \Psi(\phi_M(\vec{a}))$ if and only if $E(\Psi(\vec{a})) \notin M$.

Here we note that for any atomic formula $P(z_1, z_2, \ldots, z_k)$ and any $\vec{c} = (c_1, c_2, \ldots, c_k) \in R^{(k)}$ the reader can easily check that $E(\neg P(\vec{c})) = 1 - E(P(\vec{c}))$. It follows from Corollary 3.2.8 that

$$R_M \models \neg P(\phi_M(\vec{c})) \quad \text{if and only if} \quad E(\neg P(\vec{c})) \notin M. \qquad (3.7)$$

Next we consider the case when the formula Ψ is equivalent to the formula $\vee_{i=1}^{k}(\neg P_i)$ where $P_1, \ldots, P_n$ are atomic formulas. For simplicity we assume that all P_i's depend on $x_1, x_2, \ldots, x_n$. Since $R_M \models \vee_{i=1}^{k}(\neg P_i(\phi_M(\vec{a})))$, $R_M \models (\neg P_i(\phi_M(\vec{a})))$ for some $1 \leq i \leq k$. Then by (3.7) we have $E(\neg P_i(\vec{a})) \notin M$. Clearly $E(\neg P_i(\vec{a})) \in H(\Psi; \vec{a}) = H$ and so $E(\neg P_i(\vec{a})) \leq E(\Psi(\vec{a})) = E(H)$. Hence $E(\Psi(\vec{a})) \notin M$.

Suppose now that the formula Ψ is equivalent to the formula $P_0 \vee \left(\vee_{i=1}^{k}(\neg P_i)\right)$ where $P_0, P_1, \ldots, P_k$ are atomic formulas. As above we assume that all P_i's depend on $x_1, x_2, \ldots, x_n$. Clearly $E(P_0(\vec{a})) \in H(\Psi; \vec{a})$ as well as $E(\neg P_i(\vec{a})) \in H(\Psi; \vec{a})$ for all $i = 1, 2, \ldots, k$. Hence $E(P_0(\vec{a}))$, $E(\neg P_i(\vec{a})) \leq E(\Psi(\vec{a}))$ and so it is enough to prove that either $E(P_0(\vec{a})) \notin M$, or $E(\neg P_i(\vec{a})) \notin M$ for some $1 \leq i \leq k$. We note that $R_M \models P_0 \vee \left(\vee_{i=1}^{k}(\neg P_i)\right)$ if and only if either $R_M \models P_0$, or $R_M \models \vee_{i=1}^{k}(\neg P_i)$. Applying the above result, we complete the consideration of the case.

Assume now that the formula Ψ is equivalent to the formula $\wedge_{i=1}^{m}\Psi_i$ where each formula Ψ_i is equivalent to either an atomic formula, or a disjunction of negations of atomic formulas, or a disjunction of an atomic formula and several negations of atomic formulas. As above we assume that all Ψ_i's depend on $x_1, x_2, \ldots, x_n$. We set $e = E(\Psi(\vec{a}))$, $e_i = E(\Psi_i(\vec{a}))$ and $v = e_1 e_2 \ldots e_m$. Since $R_M \models \wedge_{i=1}^{m}\Psi_i(\phi_M(\vec{a}))$, $R_M \models \Psi_i(\phi_M(\vec{a}))$ for all $i = 1, 2, \ldots, m$ as well. By the above result we then have $e_i \notin M$ for all i and so $v \notin M$. Note that $v \leq e_i$ and so $Ru \models \Psi_i(u\vec{a})$ for all $0 < u \leq v$. Thus $Ru \models \Psi(u\vec{a})$ whence $v \in H(\Psi; \vec{a})$, i.e., $v \leq e$. Now it follows that $e \notin M$.

Next consider the case when the formula Ψ is equivalent to the formula $(\exists x_{n+1})\Phi(x_1, x_2, \ldots, x_{n+1})$ where Φ is such that for all $\vec{c} = (c_1, c_2, \ldots, c_{n+1}) \in R^{(n+1)}$ the relation $R_M \models \Phi(\phi_M(\vec{c}))$ implies that $E(\Phi(\vec{c})) \notin M$, and Φ is a Horn formula. Since $R_M \models (\exists x_{n+1})\Phi(\phi_M(\vec{a}), x_{n+1})$, there exists an element $a_{n+1} \in R$ such that $R_M \models \Phi(\phi_M(\vec{a}'))$, where $\vec{a}' = (a_1, a_2, \ldots, a_{n+1})$, and so $E(\Phi(\vec{a}')) \notin M$. Clearly $E(\Phi(\vec{a}')) \in H(\Psi; \vec{a})$. Hence $E(\Phi(\vec{a}')) \leq E(\Psi(\vec{a}))$ and so $E(\Psi(\vec{a})) \notin M$.

Finally assume that the formula Ψ is equivalent to the formula $(\forall x_{n+1})\Phi(x_1, x_2, \ldots, x_{n+1})$ where again Φ is such that for all $\vec{c} = (c_1, c_2, \ldots, c_{n+1}) \in R^{(n+1)}$ the relation $R_M \models \Phi(\phi_M(\vec{c}))$ implies that $E(\Phi(\vec{c})) \notin M$ and Φ is a Horn formula. We set

$$W \ = \ \{w \in B^* \mid \quad \text{there exists} \quad a_w \in R \quad \text{such that for every}$$

$$v \in B^*, v \leq w \quad \text{there exists} \quad u \in B^*, u \leq v,$$
$$\text{with the property} \quad uR \models \neg\Phi(ua_1, ua_2, \ldots, ua_n, ua_w))\}$$

Note that for $e \in B$ and $w \in W$ the relation $ew \neq 0$ implies that $ew \in W$ (with $a_{ew} = ea_w$). Let V be a maximal orthogonal subset of $W \cup \{0\}$. By Remark 3.1.5 we have $E(W) = E(V) = \sum_{v \in V}^{\perp} v$. We set $a_0 = 0$, $a = \sum_{v \in V}^{\perp} a_v v$ and $e = E(\Phi(a_1, a_2, \ldots, a_n, a))$. Since

$$R_M \models (\forall x_{n+1})\Phi(\phi_M(a_1), \ldots, \phi_M(a_n), x_{n+1}),$$

we have in particular that $R_M \models \Phi(\phi_M(a_1), \ldots, \phi_M(a_n), \phi_M(a))$. Then by our assumption

$$e = E(\Phi(a_1, a_2, \ldots, a_n, a)) \notin M.$$

Now we suppose that $eW \neq 0$. Since V is a maximal orthogonal subset of W, $ev \neq 0$ for some $v \in V$. Recalling that Φ is a Horn formula, we infer from Lemma 3.2.9 that for every nonzero u, $u \leq ev \leq e = E(\Phi(a_1, a_2, \ldots, a_n, a))$, we have that

$$uR \models \Phi(ua_1, ua_2, \ldots, ua_n, ua).$$

Note that $uea_v = ua_v = uva_v = uva = ua$. On the other hand by the definition of W, there exist a nonzero idempotent $u \leq ev$ such that

$$uR \models \neg\Phi(ua_1, ua_2, \ldots, ua_n, ua),$$

a contradiction. Hence $eW = 0$.

Next we suppose that $E(\Phi(a_1, a_2, \ldots, a_n, b))e \neq e$ for some $b \in R$. Then

$$u = e(1 - E(\Phi(a_1, a_2, \ldots, a_n, b)) \neq 0$$

and

$$uE(\Phi(a_1, a_2, \ldots, a_n, b)) = 0.$$

Consider any $0 \neq u' \leq u$. Clearly $u'E(\Phi(a_1, a_2, \ldots, a_n, b)) = 0$ and so $u' \notin H(\Phi; a_1, a_2, \ldots, a_n, b)$. By the definition of the set $H(\Phi; a_1, a_2, \ldots, a_n, b)$ it follows that

$$u''R \models \neg\Phi(u''a_1, \ldots, u''a_n, u''b)$$

for some $0 \neq u'' \leq u'$. Recalling the definition of the set W, we conclude that $u \in W$ (with $a_u = b$). But $eu = u \neq 0$ in contradiction with $eW = 0$. Therefore $E(\Phi(a_1, a_2, \ldots, a_n, b))e = e$ for all $b \in R$ and so

$$eR \models (\forall x_{n+1})\Phi(ea_1, ea_2, \ldots, ea_n, x_{n+1}).$$

Hence $e \in H(\Psi; \vec{a})$ and $e \leq E(\Psi(\vec{a}))$. Recalling that $e \notin M$, we conclude that $E(\Psi(\vec{a})) \notin M$. According to the definition of Horn formulas the proof is complete.

Let R be an orthogonally complete Ω-Δ-ring. A first order formula $\Phi(x_1, x_2, \ldots, x_n)$ of signature Ω-Δ is called *hereditary* if for all $0 \neq u \leq v \in B$ and $a_1, a_2, \ldots, a_n \in R$ the relation $vR \models \Phi(va_1, \ldots, va_n)$ implies that $uR \models \Phi(ua_1, \ldots, ua_n)$. Further a hereditary formula Φ is said to be *strictly hereditary* if for all $0 \neq v \in B$ and $a_1, a_2, \ldots, a_n \in R$ the relation $vR \models \Phi(va_1, \ldots, va_n)$ implies that there exist $b_1, b_2, \ldots, b_n \in R$ such that $R \models \Phi(b_1, \ldots, b_n)$ and $vb_i = va_i$ for all i.

Example Let $R = F \oplus F$ where F is a field. Then the formula $\Psi = (\forall x)(\forall y)\|xy \neq 0\| \vee \|x = 0\| \vee \|y = 0\|$ is hereditary but is not strictly hereditary.

Corollary 3.2.11 *Let R be an orthogonally complete Ω-Δ-ring, $\vec{a} = (a_1, a_2, \ldots, a_n) \in R^{(n)}$, $M \in Spec(B)$, $R_M = R/RM$ and $\phi_M : R \to R_M$ the canonical projection. Further let $\Psi(x_1, \ldots, x_n)$ be a hereditary formula of signature Ω-Δ such that $\neg\Psi$ is a Horn formula. Suppose that $vR \models \Psi(va_1, \ldots, va_n)$ for some $v \notin M$. Then*

$$R_M \models \Psi(\phi_M(a_1), \ldots, \phi_M(a_n)).$$

Proof. If $R_M \models \neg\Psi(\phi_M(a_1), \ldots, \phi_M(a_n))$, then by Theorem 3.2.10 we have $e = E(\neg\Psi(\vec{a})) \notin M$. Hence $ev \neq 0$ and by Lemma 3.2.9 we have

$$evR \models \neg\Psi(ev\vec{a}).$$

On the other hand since Ψ is hereditary and $vR \models \Psi(v\vec{a})$, $evR \models \Psi(ev\vec{a})$ as well, a contradiction. Thus $R_M \models \Psi(\phi_M(\vec{a}))$.

Some important subsets of rings (for example, the center, the right singular ideal, the Jacobson radical) are defined by first order formulas in the following sense. Let $\Psi(x)$ be a first order formula of signature Ω-Δ. We set

$$\mathcal{S}_\Psi(R) = \{r \in R \mid R \models \Psi(r)\}.$$

Corollary 3.2.12 *Let R be an orthogonally complete Ω-Δ-ring, $M \in Spec(B)$, $R_M = R/RM$ and $\phi_M : R \to R_M$ the canonical projection. Further let $\Psi(x)$ be a strictly hereditary Horn formula of signature Ω-Δ such that $\neg\Psi$ is a Horn formula. Then $\phi_M(\mathcal{S}_\Psi(R)) = \mathcal{S}_\Psi(R_M)$.*

Proof. If $a \in \mathcal{S}_\Psi(R)$, then $R \models \Psi(a)$ and so by Corollary 3.2.11 $R_M \models \Psi(\phi_M(a))$. Hence $\phi_M(a) \in \mathcal{S}_\Psi(R_M)$ and

$$\phi_M(\mathcal{S}_\Psi(R)) \subseteq \mathcal{S}_\Psi(R_M).$$

On the other hand if $\phi_M(b) \in \mathcal{S}_\Psi(R_M)$, then $R_M \models \Psi(\phi_M(b))$ and so by Theorem 3.2.10 $e = E(\Psi(b)) \notin M$ and $eR \models \Psi(eb)$. Since Ψ is strictly hereditary, there exists an element $d \in R$ such that $ed = eb$ and $R \models \Psi(d)$. Therefore $d \in \mathcal{S}_\Psi(R)$. Since $e \notin M$ and $eb = ed$, $\phi_M(d) = \phi_M(b)$ and so $\phi_M(\mathcal{S}_\Psi(R)) \supseteq \mathcal{S}_\Psi(R_M)$ which completes the proof.

Corollary 3.2.13 *Let R be an orthogonally complete ring with center $Z(R)$ and right singular ideal $Z_r(R)$, $M \in Spec(B)$, $R_M = R/RM$ and $\phi_M : R \to R_M$ the canonical projection. Then $\phi_M(Z(R)) = Z(R_M)$ and $\phi_M(Z_r(R)) = Z_r(R_M)$.*

Proof. Consider the formulas

$$\begin{aligned}\Phi(x) &= (\forall y)\|xy = yx\|,\\ \Psi(x) &= (\forall y)(\exists z)(\|y = 0\| \vee \|yz \neq 0\|) \wedge \|xyz = 0\|.\end{aligned}$$

Clearly $Z(R) = \mathcal{S}_\Phi(R)$ and $Z_r(R) = \mathcal{S}_\Psi(R)$. Since $Z(eR) = eZ(R)$ and $Z_r(eR) = eZ_r(R)$ for all $0 \neq e \in B$, both formulas Φ and Ψ are strictly hereditary. Obviously they are Horn formulas. Further

$$\begin{aligned}\neg\Phi(x) &= (\exists y)\|xy \neq yx\|,\\ \neg\Psi(x) &= (\exists y)(\forall z)(\|y \neq 0\| \wedge \|yz = 0\|) \vee \|xyz \neq 0\|\\ &= (\exists y)(\forall z)(\|y \neq 0\| \vee \|xyz \neq 0\|)\\ &\quad \wedge(\|yz = 0\| \vee \|xyz \neq 0\|)\end{aligned}$$

are Horn formulas. By Corollary 3.2.12

$$Z(R_M) = \mathcal{S}_\Phi(R_M) = \phi_M(\mathcal{S}_\Phi(R)) = \phi_M(Z(R)).$$

Analogously $Z_r(R_M) = \phi_M(Z_r(R))$.

Lemma 3.2.14 *Let R be an orthogonally complete ring, $M \in Spec(B)$, $R_M = R/RM$ and $\phi_M : R \to R_M$ the canonical projection. Further, let D be an orthogonally complete dense right ideal of R. Then $\phi_M(D)$ is a dense right ideal of R_M.*

Proof. Consider the sentence

$$\Phi = (\forall x)(\forall y)(\exists z)(\|x = 0\| \vee \|xz \neq 0\|) \wedge \|yz \in D\|.$$

Since eD is a dense right ideal of eR for all $0 \neq e \in B$, Φ is a hereditary formula. Further,

$$\begin{aligned}\neg\Phi &= (\exists x)(\exists y)(\forall z)(\|x \neq 0\| \wedge \|xz = 0\|) \vee \|yz \notin D\|\\ &= (\exists x)(\exists y)(\forall z)(\|x \neq 0\| \vee \|yz \notin D\|)\\ &\quad \wedge(\|xz = 0\| \vee \|yz \notin D\|)\end{aligned}$$

is a Horn formula. Now by Corollary 3.2.11 we have

$$\begin{aligned} R_M \models\ & (\forall x)(\forall y)(\exists z)(\|x = 0\| \vee \|xz \neq 0\|) \\ & \wedge(\|yz \in \phi_M(D)\|) \end{aligned}$$

and so $\phi_M(D)$ is a dense right ideal of R_M.

Here we note that if R is an orthogonally complete ring with maximal right ring of quotients $Q = Q_{mr}(R)$ and $M \in Spec(R)$, then $(QM) \cap R = RM$ by Remark 3.2.2**(ii)**. Therefore we can identify the ring $R_M = R/RM$ with the subring $(R + QM)/QM$ of Q/QM.

Theorem 3.2.15 *Let R be an orthogonally complete ring with extended centroid C and $Q = Q_{mr}(R)$, $B = B(C)$, $M \in Spec(B)$, $Q_M = Q/QM$ and $\phi_M : Q \to Q_M$ the canonical projection. Then:*

(i) $Q_M \subseteq Q_{mr}(R_M)$;
(ii) $\phi_M(Q_r) \subseteq Q_r(R_M)$;
(iii) $\phi_M(Q_s) \subseteq Q_s(R_M)$;
(iv) The extended centroid of R_M is equal to $\phi_M(C)$.

Proof. Let $q \in Q$ and $D = (q : R)_R$. By Lemma 3.1.19 D is an orthogonally complete dense right ideal of R. According to Lemma 3.2.14, $\phi_M(D)$ is a dense right ideal of R_M. Clearly $\phi_M(q)\phi_M(D) \subseteq R_M$. Suppose that $\phi_M(q)\phi_M(D) = 0$. Then $\phi_M(qD) = 0$. By Lemma 3.1.18 qD is an orthogonally complete subset of R and so $eqD = 0$ for $e = 1 - E(qD) \in B \setminus M$ (see Corollary 3.2.4). Since D is a dense right ideal of R, we conclude that $eq = 0$ and hence $\phi_M(q) = \phi_M(eq) = 0$. Therefore for any $x \in Q_M$ we have proved that $K_x = (x : R_M)_{R_M}$ is a dense right ideal of R_M and $xK \neq 0$. Then the mapping $x \mapsto [l_x; K_x]$, where l_x is the left multiplication by x, gives an embedding of Q_M into $Q_{mr}(R_M)$. Statements **(ii)** and **(iii)** are proved analogously.

(iv) Since $Q_M \subseteq Q_{mr}(R_M)$, it is enough to prove that Q_M is centrally closed. The mapping $E : Q \to Q$, $q \mapsto E(q)$, defines an unary operation on Q. By Theorem 2.3.9**(ii)** $E(eq) = eE(q)$ for all $e \in B$, $q \in Q$. Hence Q is an orthogonally complete Ω-ring of signature $\{0, +, -, \cdot, E\}$. The rule $E(\phi_M(q)) = \phi_M(E(q))$, $q \in Q$, defines an Ω-ring structure on Q_M. For all $x \in Q_M$, clearly $E(x) \in \{0, 1\}$, and $E(x) = 0$ if and only if $x = 0$. Consider the formulas

$$\begin{aligned}\Phi(x,y) &= \{(\forall z)\|xzy = yzx\|\} \Rightarrow \\ &\quad \{(\exists c)\|E(x)y = cx\| \wedge \|c \in C\|\} \\ &= (\forall z)(\exists c)\{\|xzy = yzx\| \Rightarrow \\ &\quad (\|E(x)y = cx\| \wedge \|c \in C\|)\} \\ &= (\forall z)(\exists c)\{\|xzy \neq yzx\| \\ &\quad \vee(\|E(x)y = cx\| \wedge \|c \in C\|)\} \quad \text{and} \\ \Psi &= (\forall x)(\forall y)\Phi(x,y).\end{aligned}$$

Then

$$\neg\Psi = (\exists x)(\exists y)(\exists z)(\forall c)\|xzy = yzx\|\wedge(\|E(x)y \neq cx\|\vee\|c \notin C\|)$$

is a Horn formula. Since eQ is centrally closed with extended centroid eC, $eQ \models \Psi$ for all $e \in B$ (see Theorem 2.3.11). Therefore Ψ is hereditary. By Corollary 3.2.11, $Q_M \models \Psi$, that is to say, for every nonzero $x, y \in Q_M$ such that $xzy = yzx$ for all $z \in Q_M$ there exists $c \in \phi_M(C)$ such that $x = cy$. Let K be the extended centroid of Q_M. Clearly $\phi_M(C) \subseteq K$. Consider any element $0 \neq k \in K$. Pick $0 \neq y \in Q_M$ such that $x = ky \in Q_M$. Clearly $xzy = yzx$ for all $z \in Q_M$ and so $x = cy$ for some $c \in \phi_M(C)$. Therefore $(k - c)y = 0$. Since $y \neq 0$ and K is a field, we infer from $k - c \in K$ that $k = c$ and so $K = \phi_M(C)$.

Now we are in a position to prove the analogs of Theorem 2.3.7 and Corollary 2.3.8 for semiprime rings. We refer the reader to the remark after Theorem 2.3.9 for the definition of $\dim_C(L)$.

Theorem 3.2.16 *Let R be a semiprime ring, $Q = Q_{mr}(R)$, $q_1, q_2, \ldots, q_n \in Q$. Set $L = \sum_{i=1}^{n} Cq_i$. Then*

$$\sum_{\sigma \in S_n} \epsilon(\sigma) q_{\sigma(1)} r_1 q_{\sigma(2)} r_2 \ldots r_{n-1} q_{\sigma(n)} = 0 \qquad (3.8)$$

for all $r_1, r_2, \ldots, r_{n-1} \in R$ (where S_n is the permutation group on n symbols) if and only if $\dim_C(L) \leq n-1$.

Proof. Let $A = O(R)$. By Remark 3.1.8 and Remark 3.1.9 the identity (3.8) holds for all $r_1, r_2, \ldots, r_{n-1} \in A$. Hence it holds also for all $r_1, r_2, \ldots, r_{n-1} \in A_M \subseteq Q_M$ where $M \in$ *Spec*(B). According to Theorem 3.2.7, A_M is a prime ring. By Theorem 3.2.15 $Q_M \subseteq Q_{mr}(A_M)$ and $\phi_M(C) = C_M$ is an extended centroid of A_M. Since A_M is a homomorphic image of A,

$$\sum_{\sigma \in S_n} \epsilon(\sigma) \phi_M(q_{\sigma(1)}) r_1 \ldots r_{n-1} \phi_M(q_{\sigma(n)}) = 0$$

for all $r_1, r_2, \ldots, r_{n-1} \in A_M$. Further, by Theorem 2.3.9 L is an injective C-module and so L is an orthogonally complete subset of Q (see Proposition 3.1.6). Consider the following formula

$$\begin{aligned} \Phi &= (\exists a_1) \ldots (\exists a_{n-1})(\forall x)(\exists c_1) \ldots (\exists c_{n-1})(\wedge_{i=1}^{n-1} \|a_i \in L\|) \\ &\quad \wedge \|x \in L\| \wedge (\wedge_{i=1}^{n-1} \|c_i \in C\|) \wedge \|x = \sum_{i=1}^{n-1} c_i a_i\|. \end{aligned}$$

Clearly Φ is a Horn formula. By Theorem 2.3.7 $Q_M \models \Phi$ for all $M \in$ *Spec*(B). Therefore $E(\Phi) \notin M$ for all $M \in$ *Spec*(B), $E(\Phi) = 1$ and $Q \models \Phi$ (see Theorem 3.2.10). The proof is complete.

Corollary 3.2.17 *Let R be a semiprime ring, $Q = Q_{mr}(R)$, $C = Z(Q)$ and $a \in Q$. Then the following conditions are equivalent:*

(i) a is an algebraic element of degree $\leq n$;

(ii) $\sum_{\sigma \in S_{n+1}} \epsilon(\sigma) a^{\sigma(0)} r_0 a^{\sigma(1)} r_1 \ldots r_{n-1} a^{\sigma(n)} = 0$ for all $r_i \in R$.

Proof. The proof is analogous to that of the above theorem. The only difference is that instead of the formula Φ we consider the following formula

$$\Psi = (\exists c_1)\dots(\exists c_n)(\wedge_{i=1}^{n}\|c_i \in C\|) \wedge \|q^n = \sum_{i=1}^{n} c_i q^{n-i}\|.$$

The last important result of this chapter is the following

Theorem 3.2.18 *Let R be an orthogonally complete Ω-Δ-ring with extended centroid C, $\Psi_i(x_1, x_2, \dots, x_n)$ Horn formulas of signature Ω-Δ, $i = 1, 2, \dots$, and $\Phi(y_1, y_2, \dots, y_m)$ a hereditary first order formula such that $\neg\Phi$ is a Horn formula. Further, let $\vec{a} = (a_1, a_2, \dots, a_n) \in R^{(n)}$, $\vec{c} = (c_1, c_2, \dots, c_m) \in R^{(m)}$. Suppose that $R \models \Phi(\vec{c})$ and for every maximal ideal M of the Boolean ring $B = B(C)$ there exists a natural number $i = i(M) > 0$ such that*

$$R_M \models \Phi(\phi_M(\vec{c})) \Rightarrow \Psi_i(\phi_M(\vec{a})).$$

Then there exist a natural number $k > 0$ and pairwise orthogonal idempotents $e_1, e_2, \dots, e_k \in B$ such that $e_1 + e_2 + \dots + e_k = 1$ and $e_i R \models \Psi_i(e_i\vec{a})$ for all $e_i \neq 0$.

Proof. By Corollary 3.2.11 $R_M \models \Phi(\phi_M(\vec{c}))$ and so for every maximal ideal M we have $R_M \models \Psi_i(\phi_M(\vec{a}))$ for some $i = i(M)$. According to Theorem 3.2.10, $v_i = E(\Psi_i(\vec{a})) \notin M$. Therefore by Lemma 3.1.21 there exist a natural number k and pairwise orthogonal idempotents $e_1, e_2, \dots, e_k$ whose sum is equal to 1 such that $e_i \leq v_i$ for all $i = 1, 2, \dots, k$. If $e_i \neq 0$, then by Lemma 3.2.9 we conclude that $e_i R \models \Psi_i(e_i\vec{a})$.

We close this chapter with an example of an application of Theorem 3.2.18. We shall extend to semiprime rings the following theorem proved by Herstein [119] for prime rings. For completeness we include a proof of Herstein's theorem.

Theorem 3.2.19 *Let R be a prime ring with a derivation $d : R \to R$ such that $x^d y^d = y^d x^d$ for all $x, y \in R$. Then either R is a commutative domain, or $d^2 = 0$.*

Proof. We set $[x, y] = xy - yx$ for all $x, y \in R$. Let D be the subring of R generated by R^d. Clearly $[x^d, D] = 0$ for all $x \in R$. Suppose that $d^2 \neq 0$. Then $a^{d^2} \neq 0$ for some $a \in R$. Let $b = a^d$. We have

$$zb^d = (zb)^d - z^d b \in D$$

for all $z \in R$. Hence

$$[x^d, uvb^d] = 0 = [x^d, vb^d]$$

for all $u, v \in R$. Now we infer that

$$0 = [x^d, uvb^d] = [x^d, u]vb^d$$

for all $v \in R$. Since $b^d \neq 0$ and R is prime, we conclude that $[x^d, u] = 0$ for all $x, u \in R$ and so $D \subseteq Z(R)$. In particular

$$[x, uvb^d] = 0 = [x, vb^d]$$

for all $x, u, v \in R$. Hence

$$0 = [x, uvb^d] = [x, u]vb^d$$

for all $x, u, v \in R$ and therefore R is commutative.

Corollary 3.2.20 *Let A be a semiprime ring with a derivation $d : A \to A$ such that $x^d y^d = y^d x^d$ for all $x, y \in A$. Further, let $R = O(A)$ be the orthogonal completion of A and $B = B(C)$ where C is the extended centroid of A. Then there exists an idempotent $e \in B$ such that eR is a commutative ring and d induce a square zero derivation on $(1 - e)R$.*

Proof. By Proposition 2.5.1 the derivation d can be extended uniquely to a derivation $d : Q_{mr}(A) \to Q_{mr}(A)$. According to Remark 3.1.16 $R^d \subseteq R$ and $e^d = 0$ for all $e \in B$. Therefore R is an orthogonally complete Ω-Δ-ring where $\Omega = \{0, +, -, \cdot, d\}$. Consider formulas

$$\begin{aligned}\Phi &= (\forall x)(\forall y)\|x^d y^d = y^d x^d\|,\\ \Psi_1 &= (\forall x)(\forall y)\|xy = yx\|,\\ \Psi_2 &= (\forall x)\|x^{d^2} = 0\|.\end{aligned}$$

Using Theorem 3.2.19, one can easily check that all the conditions of Theorem 3.2.18 are fulfilled. Hence there exist two orthogonal idempotent e_1 and e_2 such that $e_1 + e_2 = 1$ and if $e_i \neq 0$, then $e_i A \models \Psi_i$, $i = 1, 2$. The proof is complete.

Chapter 4

Primitive Rings

4.1 Rings of Quotients

A ring R is *(left) primitive* if there exists a faithful irreducible left R-module V. This is equivalent to saying that there is an abelian group V for which R is a subring of $End(V)$ acting irreducibly on V (i.e., V has no R-invariant subgroups). We will generally find it useful to adopt this latter approach. For R a subring of $E = End(V)$ the set

$$N(R) = N_E(R) = \{t \in End(V) \mid tr = rt \quad \text{for all} \quad r \in R\}$$

is called the *commuting ring of* R. We consider the ring $D = End({}_RV)$ as acting from the right on V. It is well-known (and easy to show) that $D = N_E(R)^\circ$ is a division ring, where $N_E(R)^\circ$ is the opposite ring of $N_E(R)$. Given V we shall call $D = End_R(V)$ the *associated division ring* of R relatively to V (in general a primitive ring may have many nonisomorphic faithful irreducible modules with corresponding nonisomorphic associated division rings). We may regard V as a left vector space over $D^\circ = N_E(R)$. Equivalently, V is a right vector space over D. In this case we may regard V as an (R, D)-bimodule. We also regard $End(V)$ as a left vector space over D° by defining:

$$(d \cdot t)v = t(v)d, \quad d \in D^\circ,\ t \in End(V),\ v \in V.$$

Clearly $R \subseteq End(V_D)$. For S a subset of V we let $[S]_D$ (or simply $[S]$ if context is clear) denote the D-subspace of V generated by S. An element $t \in End(V)$ is said to be of *finite D-rank* in case $[tV]_D$ is finite dimensional over D.

A right primitive ring is defined in a similar fashion and the preceding remarks have their analogous counterparts in this situation.

We begin by showing that for primitive rings the symmetric ring of quotients is reasonably well-behaved. The following result is due to Whelan [275].

Theorem 4.1.1 *If R is primitive then $Q_s(R) \subseteq End(V_D)$ (hence $Q_s(R)$ is also primitive).*

Proof. We set $Q_s = Q_s(R)$. Let $q \in Q_s$, $v \in V$, and let I and J be nonzero ideals of R such that qI, Iq, Jq, qJ are all contained in R. Since $V = IV = JV$ we may write $v = \sum_{i=1}^n a_i v_i = \sum_{j=1}^m b_j w_j$, $a_i \in I$, $b_j \in J$, $v_i, w_j \in V$. For $r \in I$ we see that

$$\begin{aligned} r\left[\sum_{i=1}^n (qa_i)v_i - \sum_{j=1}^m (qb_j)w_j\right] &= \sum_{i=1}^n r(qa_i)v_i - \sum_{j=1}^m r(qb_j)w_j \\ &= (rq)\left[\sum_{i=1}^n a_i v_i - \sum_{j=1}^m b_j w_j\right] = 0 \end{aligned}$$

making use of $rq \in R$. It follows that $\sum_{i=1}^n (qa_i)v_i = \sum_{j=1}^m (qb_j)w_j$. What we have just established shows first of all that

$$\Phi_q : \sum_{i=1}^n (a_i)v_i \mapsto \sum_{i=1}^n (qa_i)v_i$$

is well-defined element of $End(V)$ and secondly that Φ is a well-defined mapping of Q_s into $End(V)$. Additivity is clear and we claim that Φ is multiplicative. Indeed, for $q_1, q_2 \in Q_s$ there exists a nonzero ideal I of R such that q_1I, Iq_1, q_2I, Iq_2 are all contained in R. Then for $a, b \in I$ we have

$$\begin{aligned}\Phi_{q_1q_2}(abv) &= [(q_1q_2)(ab)]\,v = (q_1\,[(q_2a)b])\,v \\ &= \Phi_{q_1}\,[q_2(ab)]\,v = \Phi_{q_1}\Phi_{q_2}(abv).\end{aligned}$$

Furthermore if $\Phi_q = 0$ then from $(Iq)IV = I(qI)V = 0$ we see that $Iq = 0$, hence $q = 0$ and so Φ is $1-1$.

Finally, for $q \in Q_s$, $d \in D$, $a \in I$, $v \in V$ we have

$$\begin{aligned}\Phi_q(avd) - (\Phi_q av)d &= (qa)(vd) - ([qa]v)d \\ &= (qa)(vd) - (qa)(vd) = 0\end{aligned}$$

since $qa \in R$. Consequently $\Phi_q \in End(V_D)$ and the theorem is proved.

As a result of Theorem 4.1.1 we may assume that $Q_s(R) \subseteq End(V_D)$. In particular the central closure RC and the C-subalgebra $A = R'C = RC + C$ are contained in $End(V_D)$. Clearly $C \subseteq D^\circ$. Since $C \subseteq End(V_D)$, we conclude that $cd = dc$ for all $d \in D^\circ$ and so $C \subseteq Z(D^\circ)$ where $Z(D^\circ)$ is the center of D°. Identifying $(D^\circ)^\circ$ with D and C° with C we summarize what we have thus shown in the following

Corollary 4.1.2 *If R is primitive then the central closure $A = R'C$ is contained in $End(V_D)$ and C is contained in the center of D.*

The following example shows that C need not be equal to the center of D.

Example. Let $F = Q(x)$ be the field of rational expressions in x, where Q is the rational number field, let σ be the automorphism of F given by $x \mapsto x + 1$, and let $E = F\!<\!y;\sigma\!>$ be the set of all Laurent series

$$\sum_{i=m}^{\infty} a_i y^i, \quad a_i = f_i(x) \in Q(x),\ m \in \mathcal{Z}$$

with componentwise addition and multiplication determined by $ya = a^\sigma y$ and its consequences. Since σ is of infinite period it is well known (and straightforward to show) that E is a division ring with center Q and maximal subfield $F = Q(x)$. We let $K = Q(x^2)$ and let R be the subring $E_{(l)}K_{(r)}$ of $End(E)$, where $E_{(l)}$ denotes the left multiplications by elements of E (i.e., $\{l_x \mid x \in E\}$) and $K_{(r)}$ the right multiplications by elements of K. R acts irreducibly on E since E is a division ring, and so R is primitive. As $E_{(l)} \cong E$ is centrally closed, $E_{(l)}K_{(r)} \cong E \otimes_Q K$ and K is the extended centroid of R. On the other hand we claim that the commuting ring $D = End_R(E)$ of R is $F_{(r)}$. Indeed, we first observe that for every $i \in \mathcal{Z}$ $x^{\sigma^i} = x + i$ and so from $(x^2)^{\sigma^i} = x^2 + 2ix + i^2$ we see that σ^i is the identity on K if and only if $i = 0$. Now let $d \in D$. Since d commutes with $E_{(l)}$ we have $d = r_b$ for some $b = \sum_{i=m}^{\infty} a_i y^i \in E$. From $ba = ab$ for all $a \in K$ we have $\sum_{i=m}^{\infty} a_i \left(a^{\sigma^i} - a\right) y^i = 0$. If $a_i \neq 0$ for some $i \neq 0$ we have the contradiction that $a^{\sigma^i} = a$ for all $a \in K$. Hence $i = 0$, which says that $b = a_0 \in F$, therefore $d = r_b \in F_{(r)}$. Since D clearly contains $F_{(r)}$ it follows that $D = F_{(r)} \cong F$ and our claim is established.

With reference to Theorem 4.1.1 one might ask if either Q_l or Q_r lies in $End(V_D)$. The following example ([133]) shows that the answer is no. Let V be a countably infinite dimensional vector space over a field F with basis $v_1, v_2, \ldots, v_n, \ldots$. Let x be the linear transformation given by $xv_1 = 0$, $xv_{i+1} = v_i$ and y the linear transformation given by $yv_i = v_{i^2+1}$. Let R be the F-subalgebra (with 1) of $End_F(V)$ generated by x and y. It can be shown that R acts irreducibly on V (hence is primitive), the commuting ring of R is F, and R is the free algebra in x and y

over F. The set $U = Rx \oplus Ry = xR \oplus yR$ is a two-sided ideal of R. Suppose first that $Q_l \subseteq End_F(V)$. Let $q \in Q_l$ be the element defined by $xq = y$, $yq = 0$. Since $q \neq 0$, $qv_j = \sum \alpha_i v_i \neq 0$ for some j. Then

$$0 = yqv_j = \sum \alpha_i y v_i = \sum \alpha_i v_{i^2+1} \neq 0,$$

a contradiction. Suppose next that $Q_r \subseteq End_F(V)$. We define $q \in Q_r$ according to $qx = x$, $qy = 0$. Then $qv_i = qxv_{i+1} = xv_{i+1} = v_i$ for all i. But a contradiction is reached since $0 = qyv_1 = qv_2 = v_2$.

For primitive rings containing minimal left ideals, however, the story is quite different, and we shall discuss this matter in section 4.4.

4.2 Density Theorems

As a consequence of Theorem 1.1.5 we begin with the celebrated Jacobson Density Theorem.

Theorem 4.2.1 *Let R be a (left) primitive ring with ${}_RV$ a faithful irreducible R-module and $D = End({}_RV)$ (thus V is an (R, D)-bimodule). Then for any positive integer n, if $v_1, \ldots, v_n$ are D-independent in V and $w_1, \ldots, w_n$ are arbitrary in V there exists $r \in R$ such that $rv_i = w_i$, $i = 1, 2, \ldots, n$.*

Proof. We set $M = V_D$, $N = {}_RV_D$, and $S = T = R$. $N = V$ is closed (by the irreducibility of ${}_RV$ and the definition of D). $T = R$ is total (again by the irreducibility of ${}_RV$). Therefore Theorem 1.1.5 may be applied. Let $v_1, v_2, \ldots, v_n$ be D-independent and $w_1, w_2, \ldots, w_n$ arbitrary in V. For each $i = 1, 2, \ldots, n$ set $J_i = \{r \in R \mid rv_j = 0,\ j \neq i\}$. Then by Theorem 1.1.5 $J_i v_i \neq 0$. But then $J_i v_i = V$ (since ${}_RV$ is irreducible) and so we may choose $r_i \in J_i$ such that $r_i v_i = w_i$. Setting $r = r_1 + r_2 + \ldots + r_n$, we have the desired conclusion.

Any division ring D is a division algebra over its center C. It follows from Zorn's Lemma that D contains a maximal subfield F (i.e., a subfield which is not a proper subfield of any other subfield of D) which necessarily contains C.

Corollary 4.2.2 *Let D be a finite dimensional division algebra over its center C, F a maximal subfield of D. Then there exists a natural number n such that $D \otimes_C F \cong M_n(F)$, $\dim_C(D) = n^2$ and $\dim_C(F) = n$.*

Proof. Let R be the subalgebra $D_{(l)}F_{(r)}$ of $End_C(D)$, where $D_{(l)}$ denotes the left multiplications by D and $F_{(r)}$ the right multiplications by F. Since D is a division ring, R acts irreducibly on D. Thus R is a primitive ring. Let $f \in End_R(D)$. As f commutes with $D_{(l)}$, $f(d) = f(l_d \cdot 1) = l_d f(1) = df(1)$ for all $d \in D$, where l_d is the left multiplication by d. Hence $f = r_{f(1)}$. Since f commutes with $F_{(r)}$, we have that $[f(1), x] = 0$ for all $x \in F$. Taking into account the maximality of F, we infer that $f(1) \in F$. Thus $End_R(D) = F$. Clearly $\dim_F(D) \leq \dim_C(D) < \infty$. By the Jacobson Density Theorem we have that $D_{(l)}F_{(r)} \cong M_n(F)$, where $n = \dim_F(D)$. According to Theorem 2.3.6, $D_{(l)}F_{(r)} \cong D \otimes_C F$. Hence $\dim_C(D) = \dim_F(D \otimes_C F) = n^2$. On the other hand

$$n^2 = \dim_C(D) = \dim_C(F)\dim_F(D) = n \dim_C(F)$$

and so $\dim_C(F) = n$. The proof is complete.

The present proof of Wedderburn's theorem on finite division rings is due to T. Nagahara and H. Tomnaga

Theorem 4.2.3 (Wedderburn) *Any finite division ring D is commutative.*

Proof. Suppose that D is not commutative. Without loss of generality we can assume that all proper subrings (which are in fact subdivision rings) are commutative. Let C be the center of D with $|C| = q$. If $d \notin C$, then $N(d) = \{x \in D \mid xd = dx\}$, being a proper subring of D, is commutative and hence contained in and therefore equal to a maximal subfield. By Corollary 4.2.2 $\dim_C(N(d)) = n$ and $\dim_C(D) = n^2$ for some $n > 1$. Therefore $|N(d)| = q^n$ and $|D| = q^{n^2}$. Set $D^* = D \setminus \{0\}$, $N(d)^* = N(d)\setminus\{0\}$, and $C^* = C\setminus\{0\}$, and let $C_x = \{zxz^{-1} \mid z \in D^*\}$ be the conjugacy class in D^* determined by x. By the above $|C_x| = |D^*|/|N(x)^*| = (q^{n^2}-1)/(q^n-1)$ for $x \notin C^*$ and $|C_x| = 1$ for $x \in C^*$. The class equation for D^* then reads

$$q^{n^2} - 1 = q - 1 + m\left[(q^{n^2} - 1)/(q^n - 1)\right], \quad m \geq 1$$

whence the contradiction that $q - 1$ is divisible by

$$(q^{n^2} - 1)/(q^n - 1) = q^{n(n-1)} + q^{n(n-2)} + \ldots + 1 > q - 1.$$

Therefore D is commutative.

Our aim in the rest of this section is to prove a useful "density" result due to Amitsur. In contrast to the Jacobson Density Theorem the situation will be (loosely speaking) that given independent linear transformations $\tau_1, \tau_2, \ldots, \tau_n$ a vector v will be found such that $\tau_1 v, \tau_2 v, \ldots, \tau_n v$ are independent. We start with

Remark 4.2.4 *Let R be primitive with commuting ring $\Delta = N(R)$ and central closure $A = R'C$. Then $A\Delta \cong A \otimes_C \Delta$.*

Proof. The map $\sum a_i \otimes d_i \mapsto \sum a_i d_i$, $a_i \in A$, $d_i \in \Delta$, is clearly a ring surjection. Suppose its kernel K is nonzero. Then by Theorem 2.3.5, $0 \neq a \otimes d \in K$ for some $a \in A$, $d \in \Delta$ which yields the contradiction $0 = adV = aV$.

Corollary 4.2.5 *Under the conditions of Remark 4.2.4 suppose that $a_1, a_2, \ldots, a_n$ are C-independent elements of A. Then $a_1, a_2, \ldots, a_n$ are also Δ-independent.*

Lemma 4.2.6 *Under the conditions of Remark 4.2.4, $A\Delta$ has a nonzero element of finite D-rank if and only if R has a nonzero element of finite D-rank, where $D = End({}_RV)$.*

Proof. Let $0 \neq t = \sum_{i=1}^{m} a_i d_i$ be an element of finite D-rank with m minimal. Necessarily the a_i's are C-independent and the d_i's are C-independent. If $m > 1$ choose (and fix) $r \in R$. Then $s = a_1 rt - tra_1 = \sum_{i=2}^{m}(a_1 ra_i - a_i ra_1)d_i$, hence $sV \subseteq a_1 rtV + tV$. Therefore s has finite D-rank and so $s = 0$ by the minimality of m. Since $A\Delta$ is a tensor product (by Remark 4.2.4) and since the d_i's are C-independent we conclude in particular that $a_1 ra_i = a_i ra_1$. Since r is arbitrary in R we arrive at the contradiction that a_1 and a_2 are C-dependent by Theorem 2.3.4. Therefore we have shown that $m = 1$, i.e., $t = a_1 d_1$. Since $a_1 V = a_1 d_1 V = tV$ we see that a_1 has finite D-rank. But $0 \neq b = a_1 r \in R$ for some $r \in R$ and so b is the required element in R of finite D-rank.

Let B be an abelian group and and let U be a left vector space over a division ring Δ. Then $M = Hom(B, U)$ is a left vector space over Δ by defining:

$$(\alpha m)(b) = \alpha m(v), \quad \alpha \in \Delta,\ m \in M,\ b \in B.$$

Theorem 4.2.7 (Amitsur's Lemma) *Let B be an abelian group, let U be a left vector space over a division ring Δ, U_0 be a finite dimensional subspace of U and let $T = \Delta t_1 + \Delta t_2 + \ldots + \Delta t_k \subseteq Hom(B, U)$, where $t_1, t_2, \ldots, t_k$ are Δ-independent elements. Suppose that T does not contain a nonzero element of finite Δ-rank. Then there exists $b \in B$ such that $t_1(b), \ldots, t_k(b)$ are Δ-independent mod (U_0).*

Proof. The proof is by induction on k. The case $k = 1$ is obvious, since the inclusion $t_1(B) \subseteq U_0$ means that t_1 is of finite Δ-rank. We assume the theorem true for $k - 1$ and show it for k. To this end we assume the theorem is *not* true. This means that for every $b \in B$ there exist elements $d_1, \ldots, d_k \in \Delta$ not all equal zero such that $\sum_{i=1}^{k} d_i t_i(b) \in U_0$. It follows that if $t_2(x), t_3(x), \ldots, t_k(x)$ are Δ-independent modulo U_0, then $t_1(x) = \sum_{i=2}^{k} \delta_i t_i(x) + u$ for some uniquely determined $u \in U_0$, $\delta_2, \ldots, \delta_k \in \Delta$. By the induction hypothesis there exists $b_1 \in B$ such that $t_2(b_1), t_3(b_1), \ldots, t_k(b_1)$ are Δ-independent modulo U_0. Hence

$$t_1(b_1) = \sum_{i=2}^{k} \alpha_i t_i(b_1) + u_1 \tag{4.1}$$

for some uniquely determined $u_1 \in U_0$, $\alpha_i \in \Delta$. It is enough to show that $(t_1 - \sum_{i=2}^{k} \alpha_i t_i)B \subseteq U_0$. To this end let $b \in B$ be an arbitrary element. We set $U_1 = U_0 + \sum_{i=2}^{k} \Delta t_i(b_1) + \sum_{j=1}^{k} \Delta t_j(b)$. Let b_2 be an arbitrary element of B such that $t_2(b_2), \ldots, t_k(b_2)$ are Δ-independent modulo U_1 (the existence of such an element follows from the induction hypothesis). In particular $t_2(b_2), \ldots, t_k(b_2)$ are Δ-independent modulo U_0 and so

$$t_1(b_2) = \sum_{i=2}^{k} \beta_i t_i(b_2) + u_2 \tag{4.2}$$

for some uniquely determined $u_2 \in U_0$, $\beta_i \in \Delta$. Setting $V_1 = [\{t_i(b_1) \mid i = 2, 3, \ldots, k\}]$ and $V_2 = [\{t_i(b_2) \mid i = 2, 3, \ldots, k\}]$, we infer from the choice of b_2 that $V_2 \cap (U_0 + V_1) = 0$ and so

$$(U_0 + V_1) \cap (U_0 + V_2) = U_0 \tag{4.3}$$

Since $t_i(b_1 + b_2) \equiv t_i(b_2) \, mod \, U_1$, $t_2(b_1 + b_2), \ldots, t_k(b_1 + b_2)$ are Δ-independent modulo U_1 and so $t_1(b_1 + b_2) = \sum_{i=2}^{k} \gamma_i t_i(b_1 + b_2) + u_3$ for some uniquely determined $u_3 \in U_0$, $\gamma_i \in \Delta$. Hence

$$t_1(b_1) - \sum_{i=2}^{k} \gamma_i t_i(b_1) = \sum_{i=2}^{k} \gamma_i t_i(b_2) - t_1(b_2) + u_3. \tag{4.4}$$

It follows from (4.1) that the left side of (4.4) belongs to $U_0 + V_1$. On the other hand by (4.2) the right side of (4.4) belongs to

$U_0 + V_2$. Now (4.3) implies that each side of (4.4) belongs to U_0. Then by (4.1) and (4.2) we conclude that $\alpha_i = \gamma_i = \beta_i$ for all $i = 2, 3, \ldots, k$. In particular

$$t_1(b_2) - \sum_{i=2}^{k} \alpha_i t_i(b_2) \in U_0. \tag{4.5}$$

Since $t_i(b+b_2) \equiv t_i(b_2)\, mod\, U_1$, $t_2(b_2+b), t_3(b_2+b), \ldots, t_k(b_2+b)$ are Δ-independent modulo U_1. Applying what we just have proved we conclude that $t_1(b_2+b) - \sum_{i=2}^{k} \alpha_i t_i(b_2+b) \in U_0$ and so by (4.5)

$$\left(t_1 - \sum_{i=2}^{k} \alpha_i t_i\right)(b) \in t_1(b_2) - \sum_{i=2}^{k} \alpha_i t_i(b_2) + U_0 = U_0.$$

With this contradiction the proof is complete.

We now let R be a primitive ring, recalling the framework that R acts densely on a vector space V_D over a division ring D, with $A = R'C \subseteq R'D^\circ \subseteq End_C(V)$. We consider V as a left D°-space and note that $t \in R'D^\circ$ has finite D°-rank if and only if it has finite D-rank. Furthermore $U \subseteq V$ is a D°-subspace if and only if it is D-subspace. If U is D-subspace, then $\dim_D(U) = \dim_{D^\circ}(U)$. Also we recall that $D^\circ = N(R)$. The following corollary of Amitsur's Lemma is crucial to our needs in the section 4.4.

Lemma 4.2.8 *Let R be a primitive ring, let $a_1, a_2, \ldots, a_n$ be C-independent elements of $A = R'C$, let U_0 be a finite dimensional D-subspace of V, and let $T = \sum_{i=1}^{n} a_i D^\circ$. Then either T contains a nonzero element of finite D-rank or there exist $v_0, v_1, \ldots, v_m, \ldots \in V$ such that $a_i v_j$, $i = 1, 2, \ldots, n$,$j = 0, 1, \ldots$, are D-independent modulo U_0.*

Proof. By Corollary 4.2.5 $a_1, a_2, \ldots, a_n$ are also D°-independent. Suppose there is no $0 \neq t \in T$ of finite D-rank. By Amitsur's Lemma one finds $v_0 \in V$ such that $a_1 v_0, a_2 v_0, \ldots, a_n v_0$ are

D°-independent modulo U_0 (and hence D-independent modulo U_0). Again by Amitsur's Lemma (here $B = U = V$ and $\Delta = D^\circ$) there exists $v_1 \in V$ such that $a_1v_1, a_2v_1, \ldots, a_nv_1$ are D-independent modulo the D-span of U_0 and $a_1v_0, a_2v_0, \ldots, a_nv_0$. Continuing in this fashion we obtain the desired result.

4.3 Primitive Rings with Nonzero Socle

Our main object in this book is the study of rings satisfying certain "generalized identities" and it will be seen in this connection that primitive rings with nonzero socle arise quite naturally. Accordingly we feel it is appropriate to present in some detail the basic facts about this class of rings. The following account is an abbreviated version of the full treatment given in [133, Chapter IV]. We will then close this section with the determination of the various rings of quotients in this situation.

We begin by discussing dual spaces. A left vector space ${}_\Delta V$ and right vector space W_Δ over a division ring Δ are called a *pair of dual spaces over* Δ if there exists a nondegenerate bilinear form on V and W (denoted by $\langle\ ,\ \rangle$):

$$\begin{aligned}
&(a) \quad \langle\ ,\ \rangle : V \times W \to \Delta;\\
&(b) \quad \langle v_1 + v_2,\ w\rangle = \langle v_1,\ w\rangle + \langle v_2,\ w\rangle,\\
&\qquad \langle v,\ w_1 + w_2\rangle = \langle v,\ w_1\rangle + \langle v,\ w_2\rangle;\\
&(c) \quad \langle \alpha v,\ w\rangle = \alpha\langle v,\ w\rangle,\\
&\qquad \langle v,\ w\alpha\rangle = \langle v,\ w\rangle\alpha;\\
&(d) \quad \langle v,\ W\rangle = 0 \quad \text{implies} \quad v = 0;\\
&(e) \quad \langle V,\ w\rangle = 0 \quad \text{implies} \quad w = 0.
\end{aligned}$$

for all $v, v_i \in V$, $w, w_i \in W$, $\alpha \in \Delta$. A map $a : {}_\Delta V \to {}_\Delta V$ has an *adjoint* $a^* : W_\Delta \to W_\Delta$ if $\langle va,\ w\rangle = \langle v,\ a^*w\rangle$ for all $v \in V$, $w \in W$. An important example of dual spaces is the pair ${}_{\Delta}V$, V^*_{Δ}, where $V^* = Hom({}_{\Delta}V, {}_{\Delta}\Delta)$ is the right vector space of linear functionals of V. Two sets of vectors $v_1, v_2, \ldots, v_k \in V$ and $w_1, w_2, \ldots, w_k \in W$ are called *dual to each other* in case $\langle v_i, w_j \rangle = \delta_{ij}$, $i, j = 1, 2, \ldots, k$. If V, W are a dual pair then W is isomorphic to a subspace W' of V^* via the map $w \mapsto \langle\ , w\rangle$ (making use of **(e)**). The Weak Density Theorem (Theorem 1.1.5) now enters the picture if we set $M = {}_{\Delta}V$, $N = {}_{\Delta}\Delta_{\Delta}$, $T = W'$, $S = \Delta$. $T = W'$ is total in view of **(d)**. Next consider $f : \Delta_{\Delta} \to \Delta_{\Delta}$. Setting $f(1) = \lambda$ we have

$$f(\gamma) = f(1 \cdot \gamma) = f(1)\gamma = \lambda\gamma$$

for all $\gamma \in \Delta$. Therefore $N = {}_{\Delta}\Delta_{\Delta}$ is closed. Now let $v_1, \ldots, v_n$ be Δ-independent in V and for each i set $J_i = \{w' \in W' \mid v_j w' = 0,\ \ j \neq i\}$. By Theorem 1.1.5 $v_i J_i \neq 0$, $i = 1, 2, \ldots, n$, and since $v_i J_i = \Delta$ we can find $w_i' \in J_i$ such that $v_i w_i' = 1$. Since $w_i' = \langle\ , w_i\rangle$ we have proved

Theorem 4.3.1 *If V and W are a pair of dual spaces over Δ and $v_1, v_2, \ldots, v_n$ are Δ-independent in V then there exists $w_1, w_2, \ldots, w_n \in W$ such that $\langle v_i, w_j \rangle = \delta_{ij}$, $i, j = 1, 2, \ldots, n$.*

We now define two sets:

$$\begin{aligned} \mathcal{L}_W(V) &= \{a \in End({}_{\Delta}V) \mid a \ \text{ has an adjoint}\}; \\ \mathcal{F}_W(V) &= \{a \in End({}_{\Delta}V) \mid a \ \text{ has an adjoint and is of} \\ &\qquad \text{finite rank}\}. \end{aligned}$$

$\mathcal{F}_W(V)$ is an ideal of the ring $\mathcal{L}_W(V)$ and may be characterized according to

Theorem 4.3.2 *$a \in \mathcal{F}_W(V)$ if and only if a is a sum of elements of the form $x \mapsto \langle x, w\rangle u$,*

Proof. Since any mapping of the form $x \mapsto \langle x, w\rangle u$ is of rank one and has an adjoint $y \mapsto w\langle u, y\rangle$, any sum of a finite number of such mappings is of finite rank and has an adjoint. Therefore it is enough to prove that any $a \in \mathcal{F}_W(V)$ is a sum of elements of the above form. Clearly $Va = \sum_{i=1}^n \Delta v_i$, where $v_1, v_2, \ldots, v_n$ are Δ-independent. By Theorem 4.3.1 there exist elements $w_1, w_2, \ldots, w_n \in W$ such that $\langle v_i, w_j\rangle = \delta_{ij}$ for all i, j. Obviously

$$va = \sum_{i=1}^{n} \langle va, w_i\rangle v_i = \sum_{i=1}^{n} \langle v, a^* w_i\rangle v_i$$

for all $v \in V$, which completes the proof.

Recall that a nonzero left ideal L of an arbitrary ring A is said to be *minimal* if its does not properly contain any nonzero left ideal of A. We continue with the following general

Proposition 4.3.3 *Let L be a minimal left ideal of a ring A. Suppose that $L^2 \neq 0$. Then there exists an idempotent $e \in L$ such that $L = Ae$. Moreover eAe is a division ring. Further, if A is a semiprime ring and $v \in A$ is an idempotent such that vAv is a division ring, then Av is a minimal left ideal of A.*

Proof. Since $L^2 \neq 0$, $Lx \neq 0$ for some $x \in L$. Then by the minimality of L we have $L = Lx$. Therefore $ex = x$ for some $e \in L$. Hence $e^2x = ex = x$ and $(e^2 - e)x = 0$. Letting $l(x)$ denote the left annihilator of x in A we infer that $e^2 - e \in l(x) \cap L$. Since $Lx \neq 0$, $L \not\subseteq l(x)$. Again by the minimality of L we have $L \cap l(x) = 0$ and $e^2 - e = 0$. Therefore e is an idempotent. Clearly $0 \neq e = e^2 \in Ae \subseteq L$ and $L = Ae$. Now let $exe \in eAe$ be any nonzero element. Then $exe = e(exe) \in Aexe$ and $0 \neq Aexe \subseteq L$. By the minimality of L we have $Aexe = L$ and in particular $yexe = e$. Hence $(eye)(exe) = e$ and exe is an invertible element of eAe. Therefore eAe is a division ring.

Suppose that v is a nonzero idempotent of a semiprime ring A such that vAv is a division ring. Let $y = av \in Av$ be a nonzero element. Being a semiprime ring A has no nontrivial right annihilator. Hence $Ay \neq 0$. Therefore $(Ay)^2 \neq 0$ and $avbav \neq 0$ for some $b \in A$. We have $vbav \neq 0$ and $vbav \in vAv$. This implies that $(vzv)(vbav) = v$ for some $z \in A$. Thus $v \in Ay$, $Av \subseteq Ay \subseteq Av$ and $Ay = Av$ which completes the proof.

Given any ring A the sum of all minimal left ideals of A is called the *left socle* of A and is denoted by $Soc_l(A)$. The notion of *right socle* is introduced analogously. We note that in general left and right socles are not necessarily equal. For example if A is the ring of upper triangular (2×2)-matrices over a field, then $Soc_l(A) \neq Soc_r(A)$. The following corollary follows immediately from Proposition 4.3.3.

Corollary 4.3.4 *Let A be a semiprime ring and $e = e^2 \in A$. Then:*

(i) *Ae is a minimal left ideal if and only if eA is a minimal right ideal of the ring A;*

(ii) *$Soc_l(A) = Soc_r(A)$.*

Remark 4.3.5 *Let A be a ring. Then $Soc_l(A)$ is an ideal of A and is a direct sum of minimal left ideals.*

Proof. For an element $a \in A$ we let r_a to be the right multiplication by a (i.e., $r_a : A \to A$, $xr_a = xa$ for all $x \in A$). Since the homomorphic image of a minimal left ideal under a right multiplication is either zero or again a minimal left ideal, we have that $Soc_l(A)a = Soc_l(A)r_a \subseteq Soc_l(A)$ and $Soc_l(A)$ is an ideal of A. Making use of Zorn's lemma we conclude that there exists a family $\{L_\gamma \mid \gamma \in \Gamma\}$ of left ideals of A maximal with respect to the property $\sum_{\gamma\in\Gamma} L_\gamma$ is direct. If L is a minimal left ideal which does not belong to $\sum_{\gamma\in\Gamma} L_\gamma$, then $L \cap \sum_{\gamma\in\Gamma} L_\gamma = 0$ and the sum $L + \sum_{\gamma\in\Gamma} L_\gamma$ is direct, in contradiction with the choice of the family $\{L_\gamma \mid \gamma \in \Gamma\}$. Thus $L \subseteq \{L_\gamma \mid \gamma \in \Gamma\}$ and $\sum_{\gamma\in\Gamma} L_\gamma = Soc_l(A)$.

An idempotent $e \neq 0$ of a semiprime ring A is called *minimal* if Ae is a minimal left ideal of A. It follows immediately from Proposition 4.3.3, that a semiprime ring A has a nonzero socle if and only if it has a minimal idempotent. Furthermore, if e is a minimal idempotent of a semiprime ring A, then eAe is a division ring.

Now let R be a prime ring with nonzero socle and let e be a minimal idempotent of R. Then $V = eR$ is a faithful irreducible right R-module and also a left vector space over $\Delta = eRe$. If $\phi \in D = End_R(V)$, then $\phi(e) = \phi(e^2) = \phi(e)e \in eRe$ and, in view of this observation, it is straightforward to show that $D \cong \Delta$ (here we are letting D act on V from the left). Thus Δ is the associated division ring of R relative to $V = eR$.

Theorem 4.3.6 *Let R be a primitive ring and let V be any faithful irreducible right R-module with associated division ring D (thus we may regard R as acting densely on ${}_DV$ in view of the Jacobson Density Theorem). Then:*

(i) $Soc(R) = \{r \in R \mid rank \quad r < \infty\}$;

(ii) $Soc(R) = Soc(H)$ (recall Theorem 4.1.1) where H is any ring such that $R \subseteq H \subseteq Q_s(R)$.

Proof. Let $S = \{r \in R \mid \text{rank} \quad r < \infty\}$. Let $a \in S$ be of rank n and let $w_1, w_2, \ldots, w_n$ be a D-basis of Va. By density for each $i = 1, 2, \ldots, n$ there exists $r_i \in R$ such that $w_j r_i = \delta_{ij} w_i$, whence $a = \sum_{i=1}^{n} ar_i$. Therefore, in order to prove **(i)**, it suffices to show that $a \in R$ has rank 1 if and only if the right ideal J generated by a is minimal. Suppose a has rank 1. Setting $W = \ker(a)$ we may write $V = W \oplus Dv$, with $Wa = 0$ and $u = va \neq 0$. Now let $0 \neq b \in J$. Since $Wb = 0$ we must have $w = vb \neq 0$. By density there exists $c \in R$ such that $wc = u$ and so $vbc = u$, which shows that $a = bc$. It follows that J is minimal. Conversely, suppose J is minimal but a has rank > 1. Then we may find two D-independent vectors va, wa in V. By density there exists $r \in R$ such that $var = 0$ but $war \neq 0$. Then

$$0 \neq ar \in L = \{y \in J \mid vy = 0\} \subset J$$

since $a \in J$ but $a \notin L$, a contradiction to the minimality of J.

To prove **(ii)** we first recall from Theorem 4.1.1 that $Q_s = Q_s(R) \subseteq End_D(V)$. Since $R \subseteq H$ it is immediate from **(i)** that $Soc(R) \subseteq Soc(H)$. Now let $q \in Soc(H)$ and let $v_1q, v_2q, \ldots, v_nq$ be a D-basis for Vq. There exists $0 \neq I \triangleleft R$ such that $Iq+qI \subseteq R$. It is easy to see that V is an irreducible right I-module and so I acts densely on V. Hence there exists $r \in I$ such that $v_iqr = v_iq$ for all $i = 1, 2, \ldots, n$. Clearly $V = \ker(q) \oplus \sum_{i=1}^{n} Dv_i$ and so $V(q - qr) = 0$. Thus $q = qr \in R$ and the proof is complete.

The next theorem shows that primitive rings with nonzero socle have many nice properties.

Theorem 4.3.7 *Let R be a primitive ring with nonzero socle, let V be any faithful irreducible right R-module (with associated division ring D), and let e be any minimal idempotent (with $\Delta = eRe$). Then:*

(i) *There are a ring isomorphism $\tau : \Delta \rightarrow D$ and a τ-semilinear isomorphism $\sigma : eR \rightarrow V$ such that σ is also a right R-module map;*

(ii) *Every nonzero right (left) ideal of R contains a minimal idempotent;*

(iii) *$Soc(R)$ is a right ideal of $End({}_DV)$;*

(iv) *$Soc(R)$ is contained in every essential right (left) ideal of R;*

(v) *$Soc(R)$ is the unique minimal ideal of R;*

(vi) *$Soc(R)$ is a simple ring;*

(vii) *$Q_{ml}(R) = Q_l(R)$;*

(viii) *$Q_{ml}(R) = End({}_\Delta eR) \cong End({}_DV)$ with $eQ_{ml}e = eRe$;*

(ix) *The extended centroid C of R is isomorphic to the center of D.*

Proof. Since V is faithful, $ve \neq 0$ for some $v \in V$. Define the mapping $\sigma : eR \to V$ by the rule $(er)^\sigma = ver$. Clearly σ is an isomorphism of right R-modules. Now we define the mapping $\tau : \Delta \to D$ setting

$$(ere)^\tau x = \left[(ere)x^{\sigma^{-1}}\right]^\sigma$$

for all $x \in V$ and $ere \in eRe$. One can easily check that all desired properties are fulfilled and so **(i)** has been established.

To prove **(ii)** let $0 \neq L$ be a right ideal of R and pick $0 \neq a \in L$. Since $aSoc(R) \neq 0$ we must have $aJ \neq 0$ for some minimal right ideal J. Then the map $x \mapsto ax$ is a right R-module isomorphism and so aJ is a minimal right ideal of R contained in L. By Proposition 4.3.3 aJ (and hence L) contains a minimal idempotent.

To prove **(iii)** let $s \in Soc(R)$ and let $t \in End({}_DV)$. By Theorem 4.3.6**(i)** s has finite rank and we choose a D-basis $v_1s, v_2s, \dots, v_ns$ for Vs. By density there exists $r \in Soc(R)$ such that $v_isr = v_ist$, $i = 1, 2, \dots, n$. From $V = \ker s \oplus \sum_{i=1}^n Dv_i$ we infer that $st = sr \in Soc(R)$.

Given any essential left ideal I of R and a minimal left ideal L we have $I \cap L \neq 0$. Since L is a minimal left ideal, $L = I \cap L \subseteq I$. Hence $I \supseteq Soc(R)$. As any nonzero ideal of a prime ring is an essential left ideal, it contains the socle. Suppose now that K is a nonzero ideal of $Soc(R)$. Since $Soc(R)$ is a nonzero ideal of the prime ring R, $K' = Soc(R)KSoc(R)$ is a nonzero ideal of R. Therefore $Soc(R) \subseteq K' \subseteq K \subseteq Soc(R)$ and $K = Soc(R)$. We have thus proved **(iv)**, **(v)** and **(vi)**.

Let $q \in Q = Q_{ml}(R)$. Then $Kq \subseteq R$ for some dense left ideal K of R. Since any dense left ideal is an essential left ideal, $K \supseteq Soc(R)$ by **(iv)**. This means that $q \in Q_l(R)$, and so $Q_{ml}(R) = Q_l(R)$, thus proving **(vii)**. Since $eR \subseteq Soc(R) \subseteq K$, we conclude that $eRq \subseteq R$. But then $eRq = e(eRq) \subseteq eR$ and hence eR is a right ideal of Q. Since $r_Q(eR) \cap R = 0$ and $r_Q(eR)$ is an ideal of Q, we conclude that $r_Q(eR) = 0$.

Therefore we may regard Q as a subring of $End({}_{\Delta}eR)$. Consider any linear transformation $t \in End({}_{\Delta}eR)$. Define the mapping $f_t : ReR \to R$ according to the rule

$$(\sum_{i=1}^{n} r_i e s_i) f_t = \sum_{i=1}^{n} r_i e(e s_i t).$$

We claim that f_t is well-defined. Indeed, let $\sum_{i=1}^{n} r_i e s_i = 0$ and set $z = \sum_{i=1}^{n} r_i e(e s_i t)$. Then $er(\sum_{i=1}^{n} r_i e s_i) = 0$ for all $r \in R$ and so

$$erz = \sum_{i=1}^{n} err_i e(e s_i t) = \left(\sum_{i=1}^{n} err_i e s_i\right) t = 0.$$

and $z = 0$, since R is prime. Therefore the mapping f_t is a well-defined homomorphism of left R-modules. Setting $q_t = [ReR;\, f_t]$, we see that $erq_t = erf_t = ert$ for all $r \in R$ and hence $q_t = t$. Therefore $Q = End({}_{\Delta}eR)$. Finally we note that the τ-semilinear isomorphism $\sigma : eR \to V$ yields $End({}_{\Delta}eR) \cong End({}_{D}V)$. By (iii) we then have $eQ \subseteq Soc(R)$ and so $eQe = eRe$. In view of Corollary 2.3.12 we conclude that $C \cong Z(\Delta)$ and $Z(\Delta)$ is isomorphic to $Z(D)$ via τ.

We now show the relationship between primitive rings with nonzero socle and bilinear forms.

Theorem 4.3.8 *Let ${}_{\Delta}V$, W_{Δ} be a dual pair of vector spaces over a division ring Δ, let R be a ring such that $\mathcal{F}_W(V) \subseteq R \subseteq \mathcal{L}_W(V)$, and let $a \mapsto a^*$ denote the adjoint map $\mathcal{L}_W(V) \to End(W_{\Delta})$. Then:*

(i) $\mathcal{F}_W(V) \neq 0$;

(ii) R acts densely on ${}_{\Delta}V$ (hence R is primitive);

(iii) The map $a \mapsto a^*$ is a ring injection and W_{Δ} is a faithful irreducible left R^*-module;

(iv) $Soc(R) = \mathcal{F}_W(V)$;

(v) $Q_s(R) = \mathcal{L}_W(V)$.

Proof. Let $\langle\ ,\ \rangle$ denote the given nondegenerate bilinear form. Clearly $\mathcal{F}_W(V) \neq 0$ since, e.g., the rank one transformation $\langle\ , w\rangle v$ has as its adjoint $w\langle v,\ \rangle$. Next let $v_1, v_2, \ldots, v_n$ be Δ-independent vectors in V and let $u_1, u_2, \ldots, u_n \in V$. By Theorem 4.3.1 there exist $w_1, w_2, \ldots, w_n \in W$ such that $\langle v_i, w_i\rangle = \delta_{ij}\ i, j = 1, 2, \ldots n$. Then

$$t = \sum_{i=1}^{n} \langle\ , w_i\rangle u_i \in \mathcal{F}_W(V)$$

is such that $v_i t = u_i$, $i = 1, 2, \ldots, n$. Thus $\mathcal{F}_W(V)$ (and hence R) acts densely on V_Δ

To prove **(iii)** first let $a, b \in R$, $v \in V$, $w \in W$ and conclude from

$$\langle v, (ab)^* w\rangle = \langle vab, w\rangle = \langle va, b^* w\rangle = \langle v, a^* b^* w\rangle$$

that $(ab)^* = a^* b^*$. If $a^* = 0$, then $\langle va, w\rangle = \langle v, a^* w\rangle = 0$ and so $a = 0$. Thus $a \mapsto a^*$ is a ring injection. Now let $0 \neq w \in W$ and y an arbitrary element of W. Picking $v \in V$ such that $\langle v, w\rangle = 1$ we note that $t = \langle\ , y\rangle v \in R$ and that $t^* = y\langle v,\ \rangle \in R^*$ is such that $t^* w = y$. It follows that W_Δ is a faithful irreducible left R^*-module.

(iv) is an immediate consequence of Theorem 4.3.6(**i**). To prove **(v)** we first pick a minimal idempotent e and an element v such that $ve \neq 0$, and write $V = veR$. By Theorem 4.3.7(**viii**) we may assume that $Q_s = Q_s(R) \subseteq End({}_\Delta V)$ and for $q \in Q_s$ we have $(ver)q = v(erq)$ where $r \in R$. Now e^* is a minimal idempotent of R^* and, in view of **(iii)**, we may analogously write $W = R^* e^* w$. We define a transformation $q^* \in End(W_\Delta)$ by $q^*(r^* e^* w) = [q(re)]^* w$, noting that $q(re) \in R$ since $re \in Soc(R)$. As the mapping $R^* e^* \to R^* e^* w$, $r^* e^* \mapsto r^* e^* w$ is an isomorphism of R^*-modules, the transformation q^* is well-defined. From

$$\begin{aligned}
&\langle verq, s^* e^* w\rangle = \langle v, (erq)^* s^* e^* w\rangle \\
&= \langle v, (erqse)^* w\rangle = \langle v, (er)^* (qse)^* w\rangle \\
&= \langle ver, q^*(s^* e^* w)\rangle
\end{aligned}$$

we see that q^* is the adjoint of q and hence $Q_s \subseteq \mathcal{L}_W(V)$. On the other hand, let $t \in \mathcal{L}_W(V) \subseteq End({}_\Delta V) = Q_{ml}(R)$ (see Theorem 4.3.7(**viii**)). Letting $S = Soc(R)$ we know from Theorem 4.3.7(**iii**) that $St \subseteq S$. To show that $t \in Q_s$ we need only show that $tS \subseteq S$. By part (**iii**) S^* is the socle of R^* and by Theorem 4.3.7(**iii**) (applied to $End(W_\Delta)$) we see that $t^*S^* \subseteq S^*$. Since $a \mapsto a^*$ is a ring injection, we conclude that $tS \subseteq S$ and the proof of the theorem is complete.

Conversely we have the important fact that the primitive rings with nonzero socle which arise in Theorem 4.3.8 are a general phenomenon.

Theorem 4.3.9 *Let R be a primitive ring with nonzero socle. Then there is a dual pair ${}_\Delta V$, W_Δ such that $\mathcal{F}_W(V) \subseteq R \subseteq \mathcal{L}_W(V)$.*

Proof. Let e be any minimal idempotent of R. We know that $V = eR$ is a faithful irreducible right R-module and R is a right primitive ring acting densely on V over $\Delta = eRe$. Setting $W = Re$ we define a bilinear form $\langle\ ,\ \rangle : V \times W \to \Delta$ by $\langle er, se\rangle = erse \in \Delta$ for all $r, s \in R$. Since R is a prime ring, $\langle\ ,\ \rangle$ is nondegenerate and so ${}_\Delta V$, W_Δ is a pair of dual spaces. Since $\langle exr, ye\rangle = exrye = \langle ex, rye\rangle$ for all $ex \in V$, $ye \in W$ and $r \in R$, any element $r \in R$ has an adjoint $r^* : ye \mapsto rye$. Hence $R \subseteq \mathcal{L}_W$. Next let $a \in \mathcal{F}_W$. By Theorem 4.3.2 there exist elements $b_i, c_i \in R$, $i = 1, 2, \ldots, n$, such that

$$exa = \sum_{i=1}^{n} \langle ex,\, b_i e\rangle ec_i = ex\left(\sum_{i=1}^{n} b_i ec_i\right) = exd$$

for all $ex \in V$, where $d = \sum_{i=1}^{n} b_i ec_i \in R$. Therefore $a = d$ and $\mathcal{F}_W \subseteq R$.

We come finally to Litoff's Theorem. Our feeling is that this theorem deserves an important place in the structure theory since it furnishes the device by which many problems in prime rings (especially those in which a "generalized identity" appears) can eventually be reduced to problems in $M_n(\Delta)$.

One first makes a general observations about dual spaces. For a subset S of W, where V, W is a pair of dual spaces over a division ring Δ, we set

$$S^{\perp} = \{v \in V \mid \langle v, S\rangle = 0\}.$$

Clearly $S^{\perp}$ is a subspace of V.

Remark 4.3.10 *If V, W are dual spaces, P and Q finite dimensional subspaces of V and W respectively, then there exist finite dimensional subspaces $P' \supseteq P$ and $Q' \supseteq Q$ of V and W respectively which are dual to each other (i.e., $\langle\ ,\ \rangle : P' \times Q' \to \Delta$ is nondegenerate).*

Proof. If $\langle\ ,\ \rangle : P \times Q \to \Delta$ is nondegenerate, then there is nothing to prove. Suppose now that there exists $q \in Q$, say, with $\langle P, q\rangle = 0$. Then choose $v \in V$ such that $\langle v, q\rangle \neq 0$ and replace P by $P_0 = P + \Delta v$. In a straightforward way one verifies that

$$Q^{\perp} \cap P_0 = Q^{\perp} \cap P$$

but

$$Q \cap P_0^{\perp} \quad \text{is a proper subspace of} \quad Q \cap P^{\perp}$$

(since $q \in P^{\perp}$ but $q \notin P_0^{\perp}$). A dimension argument shows that this process must stop in a finite number of steps, and so the remark is established.

We are now in a position to prove

Theorem 4.3.11 (Litoff's Theorem) *Let R be a primitive ring with nonzero socle $H = Soc(R)$, let $b_1, b_2, \dots, b_m \in H$ and let s be a positive integer $\leq \max\{rank(h) \mid h \in H\}$. Then there exists an idempotent e in H such that $b_1, b_2, \dots, b_m \in eRe$ and the ring eRe is isomorphic to $n \times n$-matrix ring over the associated division ring Δ of R, where $n \geq s$ is the Δ-rank of e.*

Proof. By assumption we may pick an element $b_{m+1} \in H$ such that $rank(b_{m+1}) \geq s$. By Theorem 4.3.9 we have $\mathcal{F}_W(V) \subseteq R \subseteq \mathcal{L}_W(V)$. According to Theorem 4.3.2 we may assume without loss of generality that $b_i = \langle\ ,\ w_i\rangle u_i$, i=1,2,...,m+1. Then the preceding observation show that $P = \sum_{i=1}^{m+1} \Delta u_i$ and $Q = \sum_{i=1}^{m+1} w_i\Delta$ are contained in finitely dimensional subspaces P' and Q' of V and W respectively such that P' and Q' are dual to each other. By Theorem 4.3.1 we may select dual bases $x_1, x_2, \ldots, x_n \in P'$ and $y_1, y_2, \ldots, y_n \in Q'$. We leave it for reader to verify that the elements $e_{ij} = \langle\ ,\ y_i\rangle x_j$ behave as matrix units and that each b_k (and more generally, each $r \in eRe$, where $e = \sum_{i=1}^{n} e_{ii}$) may be written in the form $\sum_{ij}\langle\ ,\ y_i\rangle\lambda_{ij}x_j$, $\lambda_{ij} \in \Delta$. Then for $e = \sum_{i=1}^{n} e_{ii}$ we have $b_k = eb_ke \in eRe \cong M_n(\Delta)$. Clearly $n \geq s$ since $b_{m+1} \in eRe$.

4.4 Generalized Pivotal Monomials

The notion of a generalized pivotal monomial was introduced by Amitsur in his 1965 paper [3], simultaneously generalizing on the one hand generalized polynomial identities and on the other hand pivotal monomials (first studied by Drazin in 1965 [99]). We give the definition in case R is a prime ring, although up to the present substantional results have only been obtained in case R is primitive. As we shall presently see (Theorem 4.4.2), a necessary and sufficient condition for a primitive ring to have a nonzero socle is that it possess a generalized pivotal monomial.

Let R be a prime ring, let $A = R'C = RC + C$, and let $S = \{a_1 = 1, a_2, \ldots, a_n\}$ be a finite set of C-independent elements of A. For a monomial of "length" m in $A{<}X{>}= A\coprod_C C{<}X{>}$ (here X is an infinite set and $C < X >$ is the free C-algebra generated by X)

$$\pi(x) = a_{i_m}x_{j_m}a_{i_{m-1}}\ldots a_{i_1}x_{j_1}a_{i_0}, \quad a_{i_k} \in S$$

the *complement* P_π is defined to be the set of all monomials $\tau(x)$ of the form

$$\tau(x) = a_{p_l} x_{q_l} a_{p_{l-1}} \dots a_{p_1} x_{q_1} a_{p_0}, \quad a_{p_k} \in S$$

subject to the following condition: if $l \leq m$ then either some $j_k \neq q_k$, $k \leq l$ or some $i_k \neq p_k$, $k < l$. For $l > m$ there is no restriction. We shall say that $\pi(x)$ is a *generalized pivotal monomial* (abbreviated *GPM*) if for each substitution $r : x_j \mapsto r_j$, $r_j \in R$, the element $\pi(r)$ lies in $\sum_{\sigma(x) \in P_\pi} A\sigma(r)$, the left ideal of A generated by all the elements $\sigma(r)$. Without loss of generality we may assume that the $\sigma(x) \in P_\pi$ involve only those x_j's which appear in $\pi(x)$ (just substitute 0 for any other variable). In the special case $S = \{1\}$ the notion of a *GPM* reduces to the notion of a *pivotal monomial* (abbreviated *PM*) in the sense of Drazin.

Our goal is to characterize primitive rings having a *GPM*. The main body of the arguments of Theorem 4.4.2 is given in the following lemma.

Lemma 4.4.1 *Let R be a primitive ring with faithful irreducible left module V, $D = End({}_R V)$, let $a_1 = 1, a_2, \dots, a_n$ be C-independent elements of $A = R'C$, and let $T = \sum_{i=1}^n a_i D^\circ$. If R has a GPM $\pi(x) = a_{i_m} x_{j_m} a_{i_{m-1}} \dots a_{i_1} x_{j_1} a_{i_0}$, then T contains a nonzero element of finite D-rank.*

Proof. If the conclusion does not hold by Lemma 4.2.8 we can find elements $v_0, v_1, \dots, v_m \in V$ such that the elements $a_i v_j$, $i = 1, 2, \dots, n$, $j = 0, 1, \dots, m$, are D-independent. For each variable x_j appearing in $\pi(x)$ (the same variable may appear in several places) we let I_j denote the set of all integers k, $0 \leq k \leq m$, for which x_j is immediately to the left of a_{i_k}. By the density of R we may define $r_j \in R$ as follows:

$$\begin{aligned} r_j a_{i_k} v_k &= v_{k+1}, \quad k \in I_j, \\ r_j a_i v_p &= 0, \quad (i, p) \neq (i_k, k), \quad k \in I_j. \end{aligned}$$

Notice in particular that $r_j a_i v_m = 0$ for all i. We now make the substitution $r : x_j \mapsto r_j$ and write

$$\pi(r) = \sum_{\sigma(x)\in P_\pi} b_\sigma \sigma(r), \quad b_\sigma \in A.$$

A careful look at how the r_j's are defined shows that $\pi(r)v_0 = a_{i_m} v_m \neq 0$ but $\sigma(r)v_0 = 0$ for each $\sigma \in P_\pi$.

We are now able to establish the main result.

Theorem 4.4.2 (Amitsur) *([3, Theorem 16]) If R is a primitive ring then R has a generalized pivotal monomial if and only if $Soc(R) \neq 0$.*

Proof. If $Soc(R) \neq 0$ we choose an idempotent e such that Re is a minimal left ideal, hence eRe is a division ring. It follows that exe is a GPM. Conversely, if R has a GPM by Lemma 4.4.1 RD contains a nonzero element of finite D-rank. Then by Lemma4.2.6 R itself contains a nonzero element of finite D-rank and the proof is complete.

As a corollary to Lemma 4.4.1 we can easily obtain Drazin's result.

Theorem 4.4.3 (Drazin, [99]) *If R is primitive, then R has a pivotal monomial if and only if $R = End_D(V)$ with $\dim_D(V) < \infty$.*

Proof. If R has a PM then the set S consists solely of the element 1 and so by Lemma 4.4.1 there exists $0 \neq d \in D$ such that d has finite D-rank. But d is invertible and so $V = dV$ is a finite dimensional left vector space over D. Conversely, if $R \cong M_n(D)$ then R is an n^2-dimensional left vector space over D. Therefore every element $t \in R$ satisfies $\sum_{i=0}^{n^2} d_i t^i = 0$, some $d_i \neq 0$, and hence one may conclude that $t^{n^2} \in Rt^{n^2+1}$. It follows that x^{n^2} is a PM for R.

4.5 Derivations

Our aim in this section is to show that if R is a primitive ring with nonzero socle whose associated division ring is finite dimensional over its center then any derivation of R which vanishes on the center must be X-inner. This result is needed in the study of generalized identities in Chapter 7.

We begin with a very special case.

Lemma 4.5.1 *Let δ be a derivation of $R = M_n(F)$, F a field, which vanishes on F. Then δ is inner.*

Proof. The proof is by induction on n. The case $n = 1$ is clear. Let $\{e_{ij} \mid i, j = 1, 2, \ldots, n\}$ denote the usual matrix units. We set $e_1 = e_{11}$, $e_2 = e_{22} + e_{33} + \ldots + e_{nn}$, and write R in its Pierce decomposition $\oplus_{i,j=1}^2 R_{ij}$, $R_{ij} = e_i R e_j$. Then

$$e_1^\delta = e_1 e_1^\delta + e_1^\delta e_1 = \alpha e_1 + a_{12} + a_{21},$$

$\alpha \in F$, $a_{ij} \in R_{ij}$, $i \neq j$. From this we see that $e_1 e_1^\delta = \alpha e_1 + a_{12}$ and $e_1^\delta e_1 = \alpha e_1 + a_{21}$. It follows that $e_1^\delta = 2\alpha e_1 + a_{12} + a_{21}$, whence $\alpha = 0$. Therefore

$$e_1^\delta = a_{12} + a_{21} = [e_1, a_{12} - a_{21}],$$

and so, by replacing δ with $\delta - ad(a_{12} - a_{21})$, we may assume without loss of generality that $e_1^\delta = 0$. Hence $e_2^\delta = (1 - e_1)^\delta = 0$ and $R_{22}^\delta \subseteq R_{22}$. By induction there exists $b \in R_{22}$ such that $a^\delta = [a, b]$ for all $a \in R_{22}$. Since $[e_1, b] = 0$ we may replace δ by $\delta - ad(b)$ and assume that $e_1^\delta = 0$ and $\delta = 0$ on R_{22}. In particular $e_{ii}^\delta = 0$, $i = 1, 2, \ldots, n$, whence $e_{1i}^\delta = (e_{11} e_{1i} e_{ii})^\delta = \lambda_i e_{1i}$, $i > 1$, and $e_{j1}^\delta = \mu_j e_{j1}$, $j > 1$. Applying δ to $e_{ji} = e_{j1} e_{1i}$, $i, j > 1$, we obtain $0 = \mu_j e_{ji} + \lambda_i e_{ji}$ and so $\lambda_i = -\mu_j$ for all $i, j > 1$. Setting $\mu = \mu_j = -\lambda_i$, $i, j > 1$ we see that

$$[e_{1i}, \mu e_1] = -\mu e_{1i} = \lambda_i e_{1i} = e_{1i}^\delta$$

and

$$[e_{j1},\, \mu e_1] = \mu e_{j1} = e_{j1}^{\delta}.$$

It is then clear that $\delta = ad(\mu e_1)$ and the proof is complete.

Corollary 4.5.2 *Let D be a finite dimensional division algebra over its center C. Then any C-linear derivation δ of D is inner.*

Proof. Let F be a maximal subfield of D. Since δ is C-linear it may be lifted to an F-linear derivation $\widehat{\delta}$ of $R = D \otimes_C F \cong M_n(F)$ (see Corollary 4.2.2). By Lemma 4.5.1

$$\widehat{\delta} = ad(\textstyle\sum a_i \otimes \lambda_i),\ \{a_i\} \subseteq D,\ \{\lambda_i\}\ C\text{-independent in}\ \ F,$$

with $\lambda_1 = 1$ (we do not assume that $a_1 \neq 0$, but it will follow from our further considerations). For $x \in D$ we see in particular from

$$x^{\delta} \otimes 1 = (x \otimes 1)^{\widehat{\delta}} = \left[x \otimes 1,\, \textstyle\sum a_i \otimes \lambda_i\right] = \textstyle\sum [x,\, a_i] \otimes \lambda_i$$

that $x^{\delta} = [x,\, a_1]$, and the proof is complete.

Theorem 4.5.3 *Let R be a centrally closed primitive ring with nonzero socle H, with extended centroid C and with faithful irreducible right R-module M. Suppose furthermore that the associated division ring $\Delta = End_R(M)$ is finite dimensional over its center. Then any C-linear derivation δ of R is X-inner.*

Proof. We shall regard $V = M \oplus M = \{(x,\, y) \mid x, y \in M\}$ as an R-module under the multiplication $(x,\, y) \circ a = (xa,\, xa^{\delta} + ya)$. We let $M_1 = (M,\, 0)$ and $M_2 = (0,\, M)$, noting that M_2 is an R-module. Since R has nonzero socle we may write $M = mK$ for some $m \in M$ and minimal right ideal K of R. Then $N = (m,\, 0) \circ K$ is an irreducible R-submodule of V which is not contained in M_2, hence $N \cap M_2 = 0$. The equation

$$(ma,\, 0) = (ma,\, ma^{\delta}) - (0,\, ma^{\delta}) = (m,\, 0) \circ a - (0,\, ma^{\delta}),$$

$a \in K$, shows that $V = N \oplus M_2$. We define an additive map $E : V \to M$ by sending $(x, y) \mapsto y$, and an R-map $F : V \to M$ by writing $V = N \oplus M_2$ and sending $n \oplus m_2 \mapsto y$, where $m_2 = (0, y)$. We set $D = E - F$, noting that D maps M_2 to 0. For $a \in R$ we see that

$$\begin{aligned} (x, y)[a, E] &= ((x, y) \circ a)\, E - ((x, y)E)\, a \\ &= (xa, xa^\delta + ya)E - ya \\ &= xa^\delta + ya - ya = xa^\delta . \end{aligned}$$

Since F is an R-map we have $(x, y)[a, F] = 0$. It follows that

$$(x, y)[a, D] = xa^\delta .$$

Now let $\overline{V} = V/M_2$. Since D maps M_2 to 0, D induces a map $\overline{D} : \overline{V} \to M$ and so we have $\overline{(x, y)}\left[a, \overline{D}\right] = xa^\delta$. We next note that the map $\nu : M \to \overline{V}$ given by $x \mapsto \overline{(x, 0)}$ is an R-isomorphism. We note that $xa^\delta = x\nu\left[a, \overline{D}\right]$ for all $x \in M$. Since ν is an R-map we may rewrite this equation as $xa^\delta = x\left[a, \nu\overline{D}\right]$. Setting $g = \nu\overline{D}$ we then have

$$a^\delta = [a, g], \quad a \in R, \tag{4.6}$$

where $g : M \to M$ is an additive map. Considering the ring $E = End(M)$ as acting from the right on M, we remark that

$$0 = \left[\lambda, a^\delta\right] = [\lambda, [a, g]] = [a, [\lambda, g]]$$

for all $\lambda \in \Delta^\circ = N_E(R)$, $a \in R$, i.e., $[\lambda, g] \in \Delta^\circ$. Thus $[\ , g]$ induces a C-linear derivation of Δ° and so by Theorem 4.3.7(**ix**) and Corollary 4.5.2 there exists $\alpha \in \Delta^\circ$ such that $[\lambda, g] = [\lambda, \alpha]$ for all $\lambda \in \Delta^\circ$. This says that $q = g - \alpha \in N_E(\Delta^\circ) = End({}_\Delta M)$, and furthermore we have

$$a^\delta = [a, q], \quad a \in R.$$

By Theorem 4.3.9 $End({}_{\Delta}M) = Q_l(R)$ (the left two sided quotient ring of R), which says that $Hq \subseteq R$. Since $H^2 = H$, $H^\delta \subseteq H$. Therefore from $a^\delta = aq - qa$, $a \in H$, we obtain $qH \subseteq R$, hence $q \in Q_s(R)$ (the symmetric ring of quotients of R). Thus we have shown that δ is X-inner and the proof is complete.

We point out that the condition that Δ be finite dimensional in Theorem 4.5.3 is needed. For example let $F = Q(t)$ be the field of rational functions over the field of rationals and let σ be the automorphism of F given by $t \mapsto t+1$. Then the fixed field of F is just Q. Now let $D = F\langle x;\sigma\rangle$ be the division ring of all Laurent series $\sum_{i=m}^{\infty} a_i x^i$, $m \in \mathcal{Z}$, $a_i \in F$, with multiplication given according to $xa = a^\sigma x$, $a \in F$. Then the center of D is Q and $\dim_Q(D) = \infty$. We leave it for the reader to check that the map $\delta : D \to D$ given by $ax^n \mapsto nax^n$ is a derivation of D which is not inner.

4.6 Involutions

We recall from section 1.1 that an *involution* $*$ of a ring R is an antiautomorphism of period 1 or 2. An element $x \in R$ is called *symmetric* if $x^* = x$ and is called *skew* if $x^* = -x$. The subset $S = S(R)$ of all symmetric elements is closed under addition and the *Jordan product* $x \circ y = xy + yx$ and the subset $K = K(R)$ of all skew elements is closed under addition and the *Lie product* $[x, y] = xy - yx$. In dealing with involutions we will always make the blanket assumption that R has no 2-torsion, hence $S \cap K = 0$ and $2R \subseteq S + K$. In case every element is divisible by 2 we have the decomposition $R = S \oplus K$. An ideal I of R such that $I^* = I$ will be called a *$*$-ideal* . For instance the socle of a primitive ring with involution is a $*$-ideal.

In this section we first prove Kaplansky's Theorem (Theorem 4.6.8) characterizing involutions of primitive rings with nonzero socle in terms of Hermitian and alternate forms. This result is then applied to give a very tight description of involutions of $M_n(C)$, C an algebraically closed field. Finally we shall present an involution version of Litoff's Theorem.

We define an involution $*$ of a prime ring R with nonzero socle to be of *transpose type* if there exists a symmetric minimal idempotent and to be of *symplectic type* if $ee^* = 0$ for any minimal idempotent $e \in R$.

Lemma 4.6.1 *Let A be a prime ring and $u, v \in A$ minimal idempotents. Then either $vu = 0$ or uAv is a division ring with an identity e and $uAv = eAe$.*

Proof. It is enough to consider the case $vu \neq 0$. Then $uavu \neq 0$ for some $a \in A$, since A is prime. We set $b = uav$. Taking into account the minimality of uA we infer from $0 \neq bu \in buA \subseteq uA$ that $buA = uA$. Multiplying both sides by v we obtain that $buAv = uAv$. Since $b \in uAv$, we conclude that $be = b$ for some $e \in uAv$. Therefore $b(e^2 - e) = 0$. Letting T denote the right annihilator of b we infer that $e^2 - e \in T \cap uA$. Since uA is a minimal right ideal and $buA \neq 0$, we have $e = e^2$. Recalling that $e \in uAv$ we obtain that $eA = uA$ by minimality of uA. Therefore e is a minimal idempotent. Analogously $Ae = Av$. Thus $eAe = uAv$.

Theorem 4.6.2 *Let R be a primitive ring with nonzero socle and involution $*$. Then the involution $*$ is either of transpose type or of symplectic type.*

Proof. Suppose that the involution $*$ is not of symplectic type. Then there exists a minimal idempotent $v \in R$ such that $vv^* \neq 0$. By Lemma 4.6.1 v^*Rv is a division ring with identity e and $v^*Rv = eRe$. Therefore eRe is a $*$-invariant subring and in particular $e^* = e$.

Our next goal is a characterization of involutions of primitive rings with a nonzero socle in terms of bilinear forms. To this end we proceed to define the following two types of forms which will be relevant. Let Δ be a division ring with involution $\alpha \mapsto \overline{\alpha}$, ${}_\Delta V$ a vector space, and $\langle\ ,\ \rangle V \times V \to \Delta$ a biadditive mapping such that

$$\langle \alpha v,\, \beta w\rangle = \alpha\langle v,\, w\rangle\overline{\beta} \qquad (4.7)$$

for all $\alpha, \beta \in \Delta$, $v, w \in V$.

We say that $\langle\ ,\ \rangle$ is *Hermitian* relative to $\alpha \mapsto \overline{\alpha}$ if

$$\langle v,\, w\rangle = \overline{\langle w,\, v\rangle} \quad \text{for all} \quad v, w \in V.$$

We say that $\langle\ ,\ \rangle$ is *alternate* if $\overline{\alpha} = \alpha$ for all $\alpha \in \Delta$, $char(\Delta) \neq 2$ and

$$\langle v,\, w\rangle = -\langle w,\, v\rangle \quad \text{for all} \quad v, w \in V.$$

We remark that if $\langle\ ,\ \rangle$ is *alternate* then Δ is necessarily a field and $\langle v,\, v\rangle = 0$ for all $v \in V$.

Of secondary importance is the notion of a *skew Hermitian* form:

$$\overline{\langle v,\, w\rangle} = -\langle w,\, v\rangle \quad \text{for all} \quad v, w \in V.$$

The reason for this is given by the following lemma.

Lemma 4.6.3 *If $\langle\ ,\ \rangle$ is a skew Hermitian form then one of the following must occur*

(i) *$\langle\ ,\ \rangle$ is alternate;*

(ii) *If $\lambda \in \Delta$ is any nonzero skew element, then the map $\sim$: $\Delta \to \Delta$ defined by $\alpha \mapsto \tilde{\alpha} = \lambda^{-1}\overline{\alpha}\lambda$ is an involution of Δ and the form $(\ ,\ )$ defined by $(v,\, w) = \langle v,\, w\rangle\lambda$ is Hermitian relative to $\alpha \mapsto \tilde{\alpha}$.*

Proof. If there are no nonzero skew elements in Δ then $\overline{\alpha} = \alpha$ for all $\alpha \in \Delta$ and $\langle\ ,\ \rangle$ is alternate. Now let $0 \neq \lambda \in \Delta$ with $\overline{\lambda} = -\lambda$. It is straightforward to check that $\alpha \mapsto \tilde{\alpha} = \lambda^{-1}\overline{\alpha}\lambda$ is an involution. The form defined by $(v, w) = \langle v, w\rangle\lambda$ is clearly biadditive. Furthermore we have

$$\begin{aligned}(\alpha v, \beta w) &= \langle \alpha v, \beta w\rangle\lambda = \alpha\langle v, w\rangle\overline{\beta}\lambda \\ &= \alpha\langle v, w\rangle\lambda(\lambda^{-1}\overline{\beta}\lambda) = \alpha(v, w)\tilde{\beta}.\end{aligned}$$

Finally, from

$$\begin{aligned}\widetilde{(v, w)} &= \widetilde{\langle v, w\rangle}\lambda = \lambda^{-1}\overline{\langle v, w\rangle\lambda}\lambda \\ &= \lambda^{-1}\overline{\lambda\langle v, w\rangle}\lambda = (-1)\{-\langle w, v\rangle\}\lambda = \langle w, v\rangle\lambda \\ &= (w, v)\end{aligned}$$

we see that $(\ ,\ )$ is Hermitian.

We make the useful observation that if $\langle\ ,\ \rangle : V \times V \to V$ is a nondegenerate biadditive mapping satisfying (4.7) then, turning V into a right Δ-space V_Δ by defining $v \cdot \alpha = \overline{\alpha}v$, we see that ${}_\Delta V$, V_Δ is a dual pair. Accordingly, the notions and results of section 4.3 are available. In particular we shall write $\mathcal{F}_V$ for $\mathcal{F}_{V_\Delta}({}_\Delta V)$ and $\mathcal{L}_V$ for $\mathcal{L}_{V_\Delta}({}_\Delta V)$. It is straightforward to verify that the mapping $a \mapsto a^*$, a^* the adjoint of a, is an involution on $\mathcal{L}_V$.

The next four results show that involutions of transpose type correspond to Hermitian forms and involutions of symplectic type correspond to alternate forms.

Proposition 4.6.4 *If R is a prime ring with nonzero socle and with involution $*$ of transpose type, then*

$$\mathcal{F}_V \subseteq R \subseteq \mathcal{L}_V$$

where ${}_\Delta V$ is a vector space with a nondegenerate Hermitian form $\langle\ ,\ \rangle$ and $*$ is the adjoint mapping relative to $\langle\ ,\ \rangle$.

Proof. Since $*$ is of transpose type, there exists a symmetric minimal idempotent e. We set $V = eR$, $\Delta = eRe$, define $\overline{ere} =$

er^*e, and define $\langle\ ,\ \rangle : V \times V \to V$ by the rule $\langle ex,\, ey\rangle = exy^*e$. It is easily verified that this is a nondegenerate Hermitian form. The property $\langle exr,\, ey\rangle = \langle ex,\, eyr^*\rangle$ shows that $*$ is the adjoint mapping re $\langle\ ,\ \rangle$ and $R \subseteq \mathcal{L}_V$. Finally, let $t = \langle\ ,\, ea\rangle eb \in \mathcal{F}_V$, $a, b \in R$. For all $r \in R$

$$ert = \langle er,\, ea\rangle eb = era^*eb$$

and so $t = a^*eb \in R$. It follows from Theorem 4.3.2 that $\mathcal{F}_V \subseteq R$, and the proposition is proved.

Conversely, we now prove

Proposition 4.6.5 *Let ${}_\Delta V$ be a vector space over a division ring Δ of char$(\Delta) \neq 2$ with a nondegenerate Hermitian form $\langle\ ,\ \rangle$ relative to $\alpha \mapsto \overline{\alpha}$, and suppose R is a $*$-invariant subring of $\mathcal{L}_W$ such that $\mathcal{F}_V \subseteq R$. Then the involution induced on R by $*$ is of transpose type.*

Proof. Suppose the involution induced on R is not of transpose type. Then by Theorem 4.6.2 it is of symplectic type, i.e., for every minimal idempotent e we have $ee^* = 0$. Let $0 \neq v \in V$ and pick $w \in V$ such that $\langle v,\, w\rangle = 1$. Then $e = \langle\ ,\, w\rangle v \in \mathcal{F}_V \subseteq R$ is a minimal idempotent. Indeed, for $x \in V$, we have

$$\begin{aligned} xe^2 &= [\langle x,\, w\rangle v]e = \langle\langle x,\, w\rangle v,\, w\rangle v \\ &= \langle x,\, w\rangle\langle v,\, w\rangle v = xe \end{aligned}$$

and so $e = e^2$. Since e is of rank one, it is a minimal idempotent. Since $e^* = \langle\ ,\, v\rangle w$, we see by assumption that

$$\begin{aligned} 0 &= vee^* = [\langle v,\, w\rangle v]e^* = \langle\langle v,\, w\rangle v,\, v\rangle w \\ &= \langle v,\, w\rangle\langle v,\, v\rangle w = \langle v,\, v\rangle w. \end{aligned}$$

Since $w \neq 0$, we conclude that $\langle v,\, v\rangle = 0$ for all $v \in V$. Linearizing, we have $\langle x,\, y\rangle + \langle y,\, x\rangle = 0$ for all $x, y \in V$. In particular

$$0 = \langle v,\, w\rangle + \langle w,\, v\rangle = 1 + \overline{\langle v,\, w\rangle} = 2,$$

in contradiction to $char(\Delta) \neq 2$.

Proposition 4.6.6 *If R is a prime ring with nonzero socle and with involution $*$ of symplectic type, then*

$$\mathcal{F}_V \subseteq R \subseteq \mathcal{L}_V$$

where ${}_\Delta V$ is a vector space with a nondegenerate alternate form $\langle\, ,\, \rangle$ and $*$ is the adjoint mapping relative to $\langle\, ,\, \rangle$.

Proof. Let e be any minimal idempotent. By assumption $ee^* = 0 = e^*e$. We set $u = e + e^*$. Clearly u is a symmetric idempotent of rank 2 and $H = uRu \cong M_2(\Delta)$ (by the Jacobson Density Theorem). Let $e_{11} = e$, $e_{22} = e^*$, e_{12}, e_{21} be a system of matrix units of H. We have

$$e_{12}^* = (e_{11}e_{12}e_{22})^* = e_{22}^*e_{12}^*e_{11}^* = e_{11}e_{12}^*e_{22}$$

and $e_{12}^* = \alpha e_{12}$ for some $\alpha \in \Delta$. Consider $v = e_{11} + e_{12}$. Since $vR = e_{11}R = eR$, v is a minimal idempotent of R. Hence

$$0 = vv^* = (e_{11} + e_{12})(e_{22} + \alpha e_{12}) = e_{12} + \alpha e_{12}$$

and $\alpha = -1$. Analogously one can show that $e_{21}^* = -e_{21}$. Define the additive mapping $\# : \Delta \to \Delta$ by the rule

$$(exe)^\# = e_{12}(exe)^*e_{21}$$

for all $exe \in eRe = \Delta$. First we note that

$$\begin{aligned}
[(exe)(eye)]^\# &= e_{12}e_{22}y^*e_{22}x^*e_{22}e_{21} \\
&= e_{12}e_{22}y^*e_{22}e_{21}e_{12}e_{22}x^*e_{22}e_{21} \\
&= (eye)^\#(exe)^\#
\end{aligned}$$

Further

$$\begin{aligned}
(exe)^{\#\#} &= [e_{12}(exe)^*e_{21}]^\# = [e_{12}x^*e_{21}]^\# \\
&= e_{12}(e_{12}x^*e_{21})^*e_{21} \\
&= e_{12}(-e_{21})x(-e_{12})e_{21} = e_{11}xe_{11} = exe
\end{aligned}$$

which means that $\#$ is an involution of the division ring Δ. Now we define the bilinear form $\langle\ ,\ \rangle$ by the rule

$$\langle ex,\, ey\rangle = exy^*e_{21}$$

for all $ex, ey \in eR$. From

$$\begin{aligned}\langle ey,\, ex\rangle^\# &= e_{12}(eyx^*e_{21})^*e_{21} = e_{12}(-e_{21})xy^*e^*e_{21}\\ &= -exy^*e_{21} = -\langle ex,\, ey\rangle\end{aligned}$$

we infer that $\langle\ ,\ \rangle$ is a skew Hermitian bilinear form. Since R is prime, this form is nondegenerate. The property $\langle exr,\, ey\rangle = \langle ex,\, eyr^*\rangle$ for all $ex, ey \in eR$ and $r \in R$ is obvious. It shows that $*$ is the adjoint mapping re $\langle\ ,\ \rangle$ and also that $R \subseteq \mathcal{L}_V$. If $t = \langle\ ,\, ea\rangle eb \in \mathcal{F}_V$, then for all $r \in R$

$$ert = \langle er,\, ea\rangle eb = era^*e_{21}eb$$

and so $t = a^*e_{21}eb \in R$. Hence $\mathcal{F}_V \subseteq R \subseteq \mathcal{L}_V$.

Suppose that $\langle\ ,\ \rangle$ is not an alternate form. It follows from Lemma 4.6.3 that the form $(\ ,\ )$ defined by $(v,\, w) = \langle v,\, w\rangle\lambda$, $\lambda^\# = -\lambda \neq 0$, is a Hermitian form relative to the involution $\alpha \mapsto \tilde{\alpha} = \lambda^{-1}\alpha^\#\lambda$. It is easy to see that $*$ remains the adjoint mapping relative to $(\ ,\ )$ and that the rings $\mathcal{L}_V$ and $\mathcal{F}_V$ remains unchanged. But now by Proposition 4.6.5, $*$ must be of transpose type, in contradiction to our hypothesis. Therefore $\langle\ ,\ \rangle$ is an alternate form and the proof is complete.

The converse of Proposition 4.6.6 is easily shown.

Proposition 4.6.7 *Let ${}_\Delta V$ be a vector space over a division ring Δ of char$(\Delta) \neq 2$ with a nondegenerate alternate form $\langle\ ,\ \rangle$, and suppose R is a $*$-invariant subring such that $\mathcal{F}_V \subseteq R \subseteq \mathcal{L}_W$. Then the involution induced on R by $*$ is of symplectic type.*

Proof. By Theorem 4.3.8 R is primitive with nonzero socle. Suppose $*$ is of transpose type, i.e., there is a symmetric minimal idempotent $e = e^* \in R$. We can then write $V = \Delta w \oplus V(1-e)$, where $we = w \neq 0$. Let $v = \alpha w + u(1-e)$ be any element of V. Then

$$\begin{aligned}\langle w,\, v\rangle &= \langle w,\, \alpha w + u(1-e)\rangle = \langle w,\, w\rangle\alpha + \langle we,\, u(1-e)\rangle \\ &= \langle w,\, u(1-e)e\rangle = 0.\end{aligned}$$

Thus $\langle w,\, V\rangle = 0$ in contradiction to nondegeneracy of $\langle\ ,\ \rangle$, and the proposition is proved.

Taken together Propositions 4.6.4, 4.6.5, 4.6.6, 4.6.7 give us

Theorem 4.6.8 (Kaplansky's Theorem) *Let R be a primitive ring with nonzero socle (and of char $\neq 2$). Then any involution of R is either of transpose type or of symplectic type. Furthermore R has an involution $*$ of transpose (resp. symplectic) type if and only if there is a vector space ${}_{\Delta}V$ with a nondegenerate Hermitian (resp. alternate) form $\langle w,\, v\rangle$ such that $\mathcal{F}_V \subseteq R \subseteq \mathcal{L}_V$ and $*$ is the adjoint map relative to $\langle w,\, v\rangle$.*

We now apply Kaplansky's Theorem to obtain a more precise determination of involutions of $End_C(V)$ ($\cong M_n(C)$) where $\dim_C(V) = n < \infty$ and C is an algebraically closed field. Although this is admittedly a rather special case we shall see in Chapter 9 that our exposition of Herstein's Lie theory of prime rings with involution ultimately reduces to this situation.

Let V be an n-dimensional vector space over a field C of characteristic $\neq 2$, and let $End_C(V)$ denote the n^2-dimensional algebra of linear transformations of V. A set $\{e_{ij}\}$, $i, j = 1, 2, \ldots, n$, of elements of $End_C(V)$ satisfying

$$e_{ij}e_{kl} = \delta_{jk}e_{il} \tag{4.8}$$

will be referred to as a *set of transformation units* . Given a basis $v_1, v_2, \ldots, v_n$ of V the mappings $\{e_{ij}\}$ given by $v_k e_{ij} = \delta_{ik}v_j$ will be called the *transformation units re* $v_1, v_2, \ldots, v_n$ and conversely, given any set of transformation units $\{e_{ij}\}$ there is a basis $v_1, v_2, \ldots, v_n$ whose transformation units are the given e_{ij} (just pick $v_1 = ve_{11} \neq 0$ and define $v_j = v_1 e_{1j}$). It follows that if $a = \sum_{ij=1}^n \alpha_{ij} e_{ij}$, $\alpha_{ij} \in C$, then $A = (\alpha_{ij})$ is the matrix of a re $v_1, v_2, \ldots, v_n$ in the sense that $v_i a = \sum_{j=1}^n \alpha_{ij} v_j$.

Two important involutions of $End_C(V)$ can now be defined. The map $\tau : \sum_{ij=1}^n \alpha_{ij} e_{ij} \mapsto \sum_{ij=1}^n \alpha_{ji} e_{ij}$ will be called the *transpose involution re* $\{e_{ij}\}$ and, if $n = 2m$ and

$$s = e_{1,2m} + e_{2,2m-1} + \ldots + e_{m,m+1} - (e_{m+1,m} + e_{m+2,m-1} + \ldots + e_{2m,1}),$$

the map $a \mapsto sa^\tau s^{-1}$ will be called the *symplectic involution re* $\{e_{ij}\}$.

Remark 4.6.9 *Let $v_1, v_2, \ldots, v_n$ and $w_1, w_2, \ldots, w_n$ be bases of V with corresponding transformation units $\{e_{ij}\}$ and $\{f_{ij}\}$. Then $f_{ij} = t^{-1} e_{ij} t$, where t is the linear transformation given by $t : v_i \mapsto w_i$.*

Let $(\ ,\ )$ be a nondegenerate symmetric or alternate form on V. A symmetric form on ${}_CV$ is just a Hermitian form in case $\overline{\alpha} = \alpha$ for all $\alpha \in C$, and thus $(v, w) = (w, v)$ for all $v, w \in V$. Given a basis $v_1, v_2, \ldots, v_n$ of V the matrix $A = (\sigma_{ij})$, where $\sigma_{ij} = (v_i, v_j)$, is called the *matrix of* $(\ ,\ )$ *re* $v_1, v_2, \ldots, v_n$. If $w_1, w_2, \ldots, w_n$ is a second basis of V (where $w_i = \sum_{j=1}^n \rho_{ij} v_j$) and B is the matrix of $(\ ,\ )$ re $w_1, w_2, \ldots, w_n$ then $B = PA\,({}^tP)$, where $P = (\rho_{ij})$ and ${}^tP$ is the transposed matrix.

Lemma 4.6.10 *If C is algebraically closed and $(\ ,\ )$ is a nondegenerate symmetric form, then there is a basis $w_1, w_2, \ldots, w_n$ of V such that the matrix of $(\ ,\ )$ re $w_1, w_2, \ldots, w_n$ is the identity $n \times n$-matrix I.*

Proof. Suppose $(v, v) = 0$ for all $v \in V$. Picking $v, w \in V$ such that $(v, w) = \alpha \neq 0$ we immediately reach the contradiction that $(v + w, v + w) = 2\alpha \neq 0$. Thus $(w, w) = \beta \neq 0$ for some w. Since C is algebraically closed we may write $\beta = \alpha^2$ for some $\alpha \in C$. Setting $w_1 = \alpha^{-1}w$ we then have $(w_1, w_1) = 1$. The map $e : v \mapsto (v, w_1)w_1$ is a projection with $V(1-e)$ orthogonal to w_1 (i.e., $(V(1-e), w_1) = 0$), and so $(\ ,\ )$ induces a nondegenerate symmetric form on $V(1-e)$. By induction $V(1-e)$ has a basis $w_2, w_3, \ldots, w_n$ such that $(w_i, w_j) = \delta_{ij}$ and the proof is complete.

Lemma 4.6.11 *If $(\ ,\ )$ is a nondegenerate alternate form then $n = 2m$ is even number and there is a basis $w_1, w_2, \ldots, w_n$ such that the matrix of $(\ ,\ )$ re $w_1, w_2, \ldots, w_n$ is $\begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$, where I_m is the identity $m \times m$-matrix.*

Proof. Choosing $v, w \in V$ such that $(v, w) = \alpha \neq 0$ we set $w_1 = \alpha^{-1}v$, $w_n = w$ and note that $(w_1, w_n) = 1$, whence $(w_n, w_1) = -1$. The map $e : v \mapsto (v, w_n)w_1 - (v, w_1)w_n$ is a projection of V on Ve with $V(1-e)$ orthogonal to w_1 and w_n, and so $(\ ,\ )$ induces a nondegenerate alternate form on $V(1-e)$. By induction, $n-2 = 2(m-1)$ is even and $V(1-e)$ has a basis $w_2, w_3, \ldots, w_{n-1}$ such that $(w_i, w_{n-i}) = 1$ for $i = 2, 3, \ldots, m$, $(w_{m+i}, w_i) = -1$ for $i = 1, 2, \ldots, m-1$ and all other products are 0. The lemma is thereby proved.

Now assume $*$ is any involution of $End_C(V)$. We shall furthermore assume $*$ acts as the identity map on C; such involutions are called involutions of the *first kind* . (Problems concerning prime rings with involutions which do not act as the identity map on the extended centroid can be frequently reduced to prime rings without involution). By Kaplansky's Theorem $*$ is the adjoint map relative to a Hermitian or alternate form $\langle\ ,\ \rangle$. Since we are assuming that $*$ is the identity map on C it follows easily that in the Hermitian case $\langle\ ,\ \rangle$ is symmetric, i.e., $\langle v, w\rangle = \langle w, v\rangle$ for all $v, w \in V$. By Lemma 4.6.10 and Lemma 4.6.11 V has a basis $w_1, w_2, \ldots, w_n$ such that the matrix

$S = (\sigma_{ij})$ of $\langle\ ,\ \rangle$ re $w_1, w_2, \ldots, w_n$ is either I (if $\langle\ ,\ \rangle$ is symmetric) or $\begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$, $n = 2m$ (if $\langle\ ,\ \rangle$ is alternate). Let $\{f_{ij}\}$ be the set of transformation units re $w_1, w_2, \ldots, w_n$ and $a \in R$. Writing $a = \sum_{ij}^n \alpha_{ij} f_{ij}$, $a^* = \sum_{ij}^n \beta_{ij} f_{ij}$ and setting $A = (\alpha_{ij})$, $B = (\beta_{ij})$ we see from the equations

$$\langle w_i a^*, w_j\rangle = \sum_k \beta_{ik}\langle w_k, w_j\rangle = \sum_k \beta_{ik}\sigma_{kj}$$

and

$$\langle w_i, w_j a\rangle = \langle w_i, \sum_k \alpha_{jk} w_k\rangle = \sum_k \sigma_{ik}\alpha_{jk}$$

that $BS = S\,({}^tA)$, i.e., $B = S\,({}^tA)\,S^{-1}$. Translated back to an equation in R this says that $a^* = s a^\tau s^{-1}$, where a^τ is the transpose involution re $\{f_{ij}\}$. If $S = I$, then $s = 1$ and $*$ is the transpose involution re $\{f_{ij}\}$ and if $S = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$, then

$$s = f_{1,2m} + \ldots + f_{m,m+1} - (f_{m+1,m} + \ldots + f_{2m,1})$$

and $*$ is the symplectic involution re $\{f_{ij}\}$. We have thus completed the proof of the following

Theorem 4.6.12 *Let $*$ be an involution of the first kind of $R = End_C(V)$, where C is an algebraically closed field. Then there is a set of transformation units $\{f_{ij}\}$ such that $*$ is either the transpose involution or the symplectic involution relative to $\{f_{ij}\}$.*

Corollary 4.6.13 *Let $*$ be an involution of $M_n(C)$ of the first kind, where C is an algebraically closed field. Then there exists a set of matrix units $\{F_{ij}\}$ in $M_n(C)$ such that $*$ is one of the following two maps:*

(a) $\sum \alpha_{ij}F_{ij} \mapsto \sum \alpha_{ij}F_{ji}$ *(transpose);*

(b) $\sum \alpha_{ij}F_{ij} \mapsto S\,(\sum \alpha_{ij}F_{ji})\,S^{-1}$, $n = 2m$ *(symplectic), where* $S = F_{1,2m} + \ldots + F_{m,m+1} - (F_{m+1,m} + \ldots + F_{2m,1})$.

Proof. This is easily seen by letting $\phi : End_C(V) \to M_n(C)$ be a C-algebra isomorphism, defining an involution $*$ on $End_C(V)$ by $a^*\phi = (a\phi)^*$, and setting $F_{ij} = f_{ij}\phi$, where $\{f_{ij}\}$ are the transformation units given by Theorem 4.6.12.

We turn our attention now to developing the analogue of Litoff's Theorem for rings with involution. In what follows R will denote a primitive ring with involution $*$ and with nonzero socle $Soc(R)$.

We start with the following general observations about spaces with a nondegenerate Hermitian or skew Hermitian bilinear form. For a subset S of V, where V is a left vector space over a division ring Δ with a nondegenerate Hermitian or skew Hermitian bilinear form $\langle\ ,\ \rangle : V \times V \to \Delta$, we set

$$S^{\perp} = \{v \in V \mid \langle v, S\rangle = 0\}.$$

Clearly $S^{\perp}$ is a subspace of V.

Remark 4.6.14 *If V is a left vector space over a division ring Δ with a nondegenerate Hermitian or skew Hermitian bilinear form $\langle\ ,\ \rangle : V \times V \to \Delta$ and P is a finite dimensional subspace of V, then there exists a finite dimensional subspace $P' \supseteq P$ such that $\langle\ ,\ \rangle|_{P'}$ is nondegenerate.*

Proof. If $\langle\ ,\ \rangle : P \times P \to \Delta$ is nondegenerate, then there is nothing to prove. Suppose now that there exists $v \in P$, say, with $\langle v, P\rangle = 0$. Then choose $w \in V$ such that $\langle v, w\rangle \neq 0$ and replace P by $P_0 = P + \Delta w$. We claim that

$$\dim_{\Delta}(P_0^{\perp} \cap P_0) < \dim_{\Delta}(P^{\perp} \cap P).$$

Indeed, let $p+\alpha w \in P_0^{\perp}$. Since $v \in P_0$ and $\langle p, v\rangle = \pm\overline{\langle v, p\rangle} = 0$,

$$0 = \langle p + \alpha w, v\rangle = \alpha\langle w, v\rangle$$

and hence $\alpha = 0$ and $p \in P^{\perp}$. On the other hand $v \notin P_0^{\perp}$ which proves the claim. A dimension argument shows that this process must stop in a finite number of steps, and so the proof is complete.

We are now in a position to prove

Theorem 4.6.15 (*-Litoff Theorem) *Let R be a primitive ring with nonzero socle $H = Soc(R)$ and with involution $*$. Let $b_1, b_2, \dots, b_m \in H$. Then there exists a symmetric idempotent e in H such that $b_i \in eRe$ for all i and the ring eRe is isomorphic to $n \times n$-matrix ring over the associated division ring Δ of R, where n is the Δ-rank of e. If $n > 1$, then the type of the restriction of the involution $*$ on the subring eRe coincides with that of the involution $*$ of the ring R.*

Proof. Taking into account Theorem 4.6.8 we can assume that there exists a left vector space V over Δ with a nondegenerate Hermitian or alternate form $\langle\ ,\ \rangle$ such that $\mathcal{F}_V(V) \subseteq R \subseteq \mathcal{L}_V(V)$ and the involution $*$ coincides with the adjoint relative to $\langle\ ,\ \rangle$. By Theorem 4.3.2 we may assume without loss of generality that $b_i = \langle\ , w_i\rangle u_i$. Then Remark 4.6.14 shows that $P = \sum_{i=1}^{m}(\Delta u_i + \Delta w_i)$ is contained in a finitely dimensional subspace Q of V such that $\langle\ ,\ \rangle|_Q$ is nondegenerate. By Theorem 4.3.1 the subspace Q has dual bases $x_1, x_2, \dots, x_n$ and $y_1, y_2, \dots, y_n$. We leave it for the reader to verify that the elements $e_{ij} = \langle\ , y_i\rangle x_j$ behave as matrix units and that each b_k (and more generally, each $r \in eRe$, where $e = \sum_{i=1}^{n} e_{ii}$) may be written in the form $\sum_{ij}\langle\ , y_i\rangle\lambda_{ij}x_j$, $\lambda_{ij} \in \Delta$. Then for $e = \sum_{i=1}^{n} e_{ii}$ we have $b_k = eb_ke \in eRe \cong M_n(\Delta)$. Let $v \in V$. Then $ve = 0$ if and only if $\sum_{i=1}^{n}\langle v, y_i\rangle x_i = 0$. Since $x_1, x_2, \dots, x_n$ are linearly independent, the last condition is equivalent to $\langle v, y_i\rangle = 0$ for all $i = 1, 2, \dots, n$. But $y_1, y_2, \dots, y_n$ is a basis of Q. Hence we have proved that $\ker(e) = Q^{\perp}$. Since $Ve = P$, it follows that

$$\langle xe, y\rangle = \langle xe, ye + y(1-e)\rangle = \langle xe, ye\rangle = \langle x, ye\rangle$$

which means that $e^* = e$. The last statement of the theorem is obvious.

We remark that clearly the symmetric idempotent e in Theorem 4.6.15 may be chosen so that the $rank_\Delta(e) \geq k$, where k is any prescribed positive integer for which $k \leq \dim_\Delta(V)$. Indeed, let e_1 denote the symmetric idempotent guaranteed by Theorem 4.6.15, take any element c of sufficiently high finite rank in $(1 - e_1)R$, and reapply Theorem 4.6.15 to the elements e_1, c to obtain the desired symmetric idempotent e.

The $*$-Litoff Theorem will prove to be useful in Chapter 9 when we shall give an exposition of Herstein's Lie theory for prime rings with involution.

4.7 Automorphisms

Our aim in this section is a description of automorphisms of primitive rings with nonzero socle whose associated division ring is finite dimensional over its center. We show that any automorphism acting on the extended centroid identically is X-inner. We start with the following easy remark.

Remark 4.7.1 *Let α be an automorphism of $R = M_n(F)$, F a field, which acts identically on F. Then α is inner.*

Proof. Let $\{e_{ij}\}$ be a set of matrix units in $M_n(F)$. Obviously $\{e_{ij}^\alpha\}$ is again a set of matrix units. By Remark 4.6.9 there exists an invertible matrix $t \in M_n(F)$ such that $e_{ij}^\alpha = t^{-1}e_{ij}t$ for all i, j which proves the remark.

Corollary 4.7.2 *Let D be a finite dimensional division algebra over its center C. Then any C-linear automorphism α of D is inner.*

Proof. Let F be a maximal subfield of D. Since α is C-linear it may be lifted to an F-linear automorphism $\widehat{\alpha}$ of $R = D \otimes_C F \cong M_n(F)$ (see Corollary 4.2.2). By Remark 4.7.1 $\widehat{\alpha} = inn(\sum a_i \otimes \lambda_i)$, $\{a_i\} \subseteq D$, $\{\lambda_i\}$ C-independent in F, with $\lambda_1 = 1$ (otherwise we replace $(\sum a_i \otimes \lambda_i)$ with $(\sum a_i \otimes \lambda_i)(1 \otimes \lambda_1)^{-1}$). For $x \in D$ we see in particular from

$$\left[\sum a_i \otimes \lambda_i\right](x^\alpha \otimes 1) = (x \otimes 1)\left[\sum a_i \otimes \lambda_i\right]$$

that $a_1 x^\alpha = x a_1$, and the proof is complete.

Theorem 4.7.3 *Let R be a primitive ring with nonzero socle, with faithful irreducible right R-module M and $\Delta = End(M_R)$. Suppose that α is an automorphism of R. Then there exist an automorphism $\tau : \Delta \to \Delta$ and a τ-semilinear automorphism S of M such that $r^\alpha = S^{-1}rS$ for all $r \in R$.*

Proof. Here we consider R as a subring of $End_\Delta(M)$. Further we consider M as an R-module M' with multiplication given by the rule $m * r = mr^\alpha$. Clearly $End(M'_R) = \Delta$. By Theorem 4.3.7 there exist an automorphism $\tau : \Delta \to \Delta$ and a τ-semilinear isomorphism $S : M \to M'$ which is an isomorphism of right R-modules as well. We have

$$(mr)S = (mS) * r = (mS)r^\alpha$$

for all $m \in M$ and $r \in R$. Hence $rS = Sr^\alpha$ and $r^\alpha = S^{-1}rS$, which completes the proof.

Theorem 4.7.4 *Let R be a centrally closed primitive ring with nonzero socle H and with extended centroid C, and let M be a faithful irreducible right R-module whose associated division ring $\Delta = End(M_R)$ is finite dimensional over its center. Then any C-linear automorphism α of R is X-inner.*

Proof. By Theorem 4.3.7(**ix**) we can identify the center of Δ with $1_\Delta C$. It follows from Theorem 4.7.3 that $r^\alpha = S^{-1}rS$ for some τ-semilinear automorphism of M. Consider $c \in C$. Since $c^\alpha = c$, $cS = Sc$. Note that $mc = cm$ for all $m \in M$. We have

$$c(mS) = (mS)c = (mc)S = (cm)S = c^\tau(mS)$$

and hence $c = c^\tau$ for all $c \in C$. Applying Corollary 4.7.2 we infer that $\tau = inn(a)$ for some $a \in \Delta$. Consider now the endomorphism $T : M \to M$ of the abelian group M given by the rule $mT = a(mS)$ for all $m \in M$. Clearly T is an automorphism. Further

$$(mr)T = a\left[(mr)S\right] = a\left[(mS)r^\alpha\right] = \left[a(mS)\right]r^\alpha = (mT)r^\alpha$$

which means that $r^\alpha = T^{-1}rT$. Moreover

$$\begin{aligned}(dm)T &= a\left[(dm)S\right] = a\left[d^\tau(mS)\right] = ad^\tau(mS)\\ &= da(mS) = d(mT)\end{aligned}$$

for all $m \in M$ and $d \in \Delta$. Therefore $T \in End({}_\Delta M)$. By Theorem 4.3.7 $End({}_\Delta M) = Q_l(R)$ and $Soc(R)$ is a right ideal of $Q_l(R)$. Clearly $Soc(R)^\alpha = Soc(R)$ and so for every $r \in Soc(R)$ we have $Tr^\alpha = rT \in Soc(R)$. Thus

$$TSoc(R) = TSoc(R)^\alpha \subseteq Soc(R)$$

and we conclude that $T \in Q_s(R)$.

This Page Intentionally Left Blank

Chapter 5

The Poincaré-Birkhoff-Witt Theorem

In this chapter we shall prove a generalization of the well-known Poincaré-Birkhoff-Witt theorem for Lie algebras. Aside from our feeling that this result is of independent interest, we have a very tangible motivation for this project. One of the central goals in this book (Chapter 7) is the study of so-called generalized identities which involve derivations (along with automorphisms and antiautomorphisms). To be specific let R be a prime ring with extended centroid C, prime subfield Φ of C, and symmetric ring of quotients Q. Letting $D = D(R) = Der(R)C + D_i$ (where D_i is the set of inner derivations of Q) we recall from Chapter 2 that D is a certain set of derivations of Q which satisfies the following properties

(i) D is a Φ-algebra;

(ii) D is a right C-space;

(iii) There is Φ-Lie algebra map $\Lambda : D \to Der(C)$;

(iv) $[\delta c,\, \mu] = [\delta,\, \mu]c + \delta c^{\hat{\mu}}$, where $\hat{\mu} = \Lambda(\mu)$, $\delta, \mu \in D$ and $c \in C$.

In case of char. p D is also closed under pth powers (in this situation D is called restricted) and there are further natural properties (which we will not mention here).

In view of this motivation, in this chapter we shall abstract the above properties and define accordingly the notion of a (restricted) differential F-Lie algebra L (F playing the role of C). For such a Lie algebra we will construct a universal enveloping algebra (which is an F-ring) and then show that it has the expected right F-basis (Theorem 5.3.6 and Theorem 5.4.5). The main tool in the proof will be the Diamond Lemma. Since there are various level of complications, depending on whether L is an F-algebra rather than just a right F-space and on whether L is restricted or not, we have chosen to divide the chapter into four separate sections (with each succeeding section building upon the previous case). In this way the reader may restrict his attention to the level of generality in which he is interested. We have also carried through our arguments in the generality where F is a commutative ring with 1 rather than just being a field, since there is no appreciable change in the arguments. In the few instances in which there is some simplification in case F is a field these matters will be pointed out.

The main results of sections 5.1 and 5.2, namely, Theorem 5.1.1, Theorem 5.2.3, are of course well-known, although the use of the Diamond Lemma in their proof may be of interest (in preparation of these sections we used some material from [19] and [20]). Theorem 5.3.6 is a special case of a more general theorem proved by homological methods in [264] whereas we have not seen Theorem 5.4.5 in the literature.

5.1 Lie Algebras

Let Φ be a commutative ring with 1. Recall that a Φ-algebra K with multiplication $(x, y) \mapsto [x, y]$ is said to be a *Lie algebra* over Φ if it satisfies the identities

$$[x, x] = 0, \quad [x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$$

for all $x, y, z \in K$. The last identity is called the *Jacobi identity.*

Further let A be an associative Φ-algebra with an identity element 1. We set $[x, y] = xy - yx$ for all $x, y \in A$. Denote by $A^{(-)}$ the additive group A with new multiplication $[\ ,\ ]$. Clearly $A^{(-)}$ is a Lie algebra over Φ.

Let K be a Lie algebra over Φ. A pair $(A; f)$ is said to be a *cover* of the Lie algebra K if A is an associative Φ-algebra with 1 and $f : K \to A^{(-)}$ is a homomorphism of Φ-algebras. A cover $(A; f)$ of the Lie algebra K is called an *enveloping algebra* of the Lie algebra K if $A = \langle K^f \rangle + \Phi \cdot 1$, where $\langle K^f \rangle$ is the subalgebra of A generated by the image K^f of the mapping f. An enveloping algebra $(U; \phi)$ of the Lie algebra K is said to be a *universal enveloping algebra* of the Lie algebra K, if for any cover algebra $(A; f)$ of the Lie algebra K there exists a (necessarily unique) homomorphism $\psi : U \to A$ of Φ-algebras with identity elements (i.e. $1^\psi = 1$) such that $\phi\psi = f$.

Two covers $(A; f)$ and $(B; g)$ of a Lie algebra K are said to be isomorphic if there exists an isomorphism $h : A \to B$ of Φ-algebras with 1 such that $fh = g$. Clearly a universal enveloping algebra of a given Lie algebra is determined uniquely up to isomorphism.

Any Lie algebra K over Φ has a universal enveloping algebra. Indeed, let $\{(A_i, f_i) \mid i \in I\}$ be a set of all pairwise non-isomorphic enveloping algebras of the Lie algebra K. We let $A = \prod_{i \in I} A_i$ be the Cartesian product of A_i, $i \in I$. Define the mapping $\phi : K \to A$ by the rule $\phi(x) = \{f_i(x)\}_{i \in I}$ for all $x \in K$. Denote by U the subalgebra of A generated by the identity element and K^ϕ. It immediately follows from our construction that $(U; \phi)$ is the universal enveloping algebra of K.

However, we are only interested in Lie algebras which are free Φ-modules. In this case we proceed to describe the universal enveloping algebra $(U(K);\rho)$ in a more tangible fashion as follows. Let X be a Φ-basis of K, $Z=\{\bar{x}\mid x\in X\}$, $S=S{<}Z{>}$ the free semigroup (with 1), and $\Phi{<}Z{>}$ the free algebra (with 1) generated by Z. Denote by L the Φ-span of Z in $\Phi{<}Z{>}$ and let $\psi: K\to L$ be the Φ-map given by $x\mapsto\bar{x}$, $x\in X$. It is clear that ψ is an isomorphism of Φ-modules, and we set $\phi=\psi^{-1}$. We now define $I=I(K)$ to be the ideal of $\Phi{<}Z{>}$ generated by all elements of the form $[u^\psi,v^\psi]-[u,v]^\psi$, $u,v\in K$, or, equivalently, $[\bar{x},\bar{y}]-[x,y]^\psi$, $x,y\in X$. Letting ν denote the projection of $\Phi{<}Z{>}$ onto $\Phi{<}Z{>}/I$, we set $\rho=\psi\nu$. The reader may then verify the straightforward details that $(\Phi{<}Z{>}/I;\rho)$ is a universal enveloping algebra of K (if $(A;f)$ is any cover of K, first lift f to a homomorphism $\sigma:\Phi{<}Z{>}\to A$ and then just check that σ sends I to 0).

Theorem 5.1.1 *Let K be a Lie algebra over Φ with universal enveloping algebra $(U(K);\rho)$. Assume that K is a free Φ-module with a well-ordered basis X. Then $U(K)$ is a free Φ-module with the basis*

$$V=\{x_1^\rho x_2^\rho\dots x_m^\rho\mid x_j\in X,\ x_1\le x_2\le\dots\le x_m\}\cup\{1\}$$

(we shall refer to V as a PBW-basis of the universal enveloping algebra $U(K)$ of the Lie algebra K).

Proof. Let Δ be the reduction system of $\Phi{<}Z{>}$, given by

$$\sigma_{yx}=\left(\bar{y}\bar{x},\bar{x}\bar{y}+[y,x]^\psi\right)\quad\text{for all}\quad y>x\in X.$$

Further let $x,y\in X$, $P,Q\in S$. We set $R=R_{P\sigma_{xy}Q}$ for $x>y$, and $R=R_{P\sigma_{yx}Q}$ for $y>x$. Then $R\left(P[\bar{x},\bar{y}]Q\right)=P[x,y]^\psi Q$.

We claim that for any $P,Q\in S$, $u_1,u_2,\dots,u_n,v_1,v_2,\dots,v_n\in L$ there exists a sequence of reductions R such that

$$R\left(\sum_{i=1}^n P[u_i,v_i]Q\right)=\sum_{i=1}^n P[u_i^\phi,v_i^\phi]^\psi Q. \tag{5.1}$$

Indeed, let $u_i = \sum_x \nu_{ix}\bar{x}$, $v_i = \sum_y \mu_{iy}\bar{y}$, where $\nu_{ix}, \mu_{ix} \in \Phi$, $x, y \in X$. Using reductions of the form $R_{P\sigma_{xy}Q}$ (or $R_{P\sigma_{yx}Q}$) we may reduce the element

$$\begin{aligned}\sum_{i=1}^{n} P[u_i, v_i]Q &= \sum_{i,x,y} \nu_{ix}\mu_{iy}P[\bar{x}, \bar{y}]Q \\ &= \sum_{i,x<y} (\nu_{ix}\mu_{iy} - \nu_{iy}\mu_{ix})P[\bar{x}, \bar{y}]Q\end{aligned}$$

to the element

$$\begin{aligned}\sum_{i,x<y} (\nu_{ix}\mu_{iy} - \nu_{iy}\mu_{ix})P[x, y]^{\psi}Q &= \sum_{i,x,y} \nu_{ix}\mu_{iy}P[x, y]^{\psi}Q \\ &= \sum_{i=1}^{n} P\left[\sum_{x} \nu_{ix}x, \sum_{y} \mu_{iy}y\right]^{\psi} Q \\ &= \sum_{i=1}^{n} P[u_i^{\phi}, v_i^{\phi}]^{\psi}Q.\end{aligned}$$

Let $w = \bar{x}_1\bar{x}_2 \ldots \bar{x}_m \in S$. The number m is called the length of w. A linear order $\leq$ is defined on S as follows: $u < v$, if either

(a) u is of smaller length than v, or

(b) u and v have the same length but u is less then v relatively to the lexicographic order.

It is clear that this ordering $\leq$ is a semigroup ordering compatible with the reduction system Δ and that it satisfies the descending chain condition.

Denote by $I = I(\Delta)$ the ideal of the algebra $\Phi{<}Z{>}$ generated by the reduction system Δ, noting that $U(K) = \Phi{<}Z{>}/I$. We will show, that all ambiguities of Δ are resolvable and the set

$$V' = \{\bar{x}_1\bar{x}_2 \ldots \bar{x}_m \mid x_j \in X,\ x_1 \leq x_2 \leq \ldots \leq x_m\} \cup \{1\}$$

is a Φ-basis of $\Phi{<}Z{>}_{irr}$.

Indeed, only the overlap ambiguity $(\sigma_{zy}, \sigma_{yx}, \bar{z}, \bar{y}, \bar{x})$, where $x, y, z \in X$ and $z > y > x$, is possible. We set

$$\begin{aligned} w &= R_{\sigma_{zy}x}(\bar{z}\bar{y}\bar{x}) - R_{z\sigma_{yx}}(\bar{z}\bar{y}\bar{x}) \\ &= \Big(\bar{y}\bar{z}\bar{x} + [z,y]^{\psi}\bar{x}\Big) - \Big(\bar{z}\bar{x}\bar{y} + \bar{z}[y,x]^{\psi}\Big) \end{aligned}$$

and

$$\begin{aligned} w' &= R_{x\sigma_{zy}}R_{\sigma_{yx}z}R_{\sigma_{zx}y}R_{y\sigma_{zx}}(w) \\ &= \bar{x}\bar{y}\bar{z} + [y,x]^{\psi}\bar{z} + \bar{y}[z,x]^{\psi} + [z,y]^{\psi}\bar{x} \\ &- \bar{x}\bar{y}\bar{z} - \bar{x}[z,y]^{\psi} - [z,y]^{\psi}\bar{y} - \bar{z}[y,x]^{\psi} \\ &= \Big[[y,x]^{\psi}, \bar{z}\Big] + \Big[\bar{y}, [z,x]^{\psi}\Big] + \Big[[z,y]^{\psi}, \bar{x}\Big]\,. \end{aligned}$$

By (5.1) there exists a sequence of reductions R such that

$$\begin{aligned} &R\Big(\Big[[y,z]^{\psi}, \bar{z}\Big] + \Big[\bar{y}, [z,x]^{\psi}\Big] + \Big[[z,y]^{\psi}, \bar{x}\Big]\Big) \\ &= [[y,x],z]^{\psi} + [y,[z,x]]^{\psi} + [[z,y],x]^{\psi}\,. \end{aligned}$$

The last expression is equal to zero by Jacobi identity. Thus

$$RR_{x\sigma_{zy}}R_{\sigma_{yx}z}R_{\sigma_{zx}y}R_{y\sigma_{zx}}(w) = 0$$

and this ambiguity is resolvable. Therefore by the *Diamond Lemma* $U(K) = \Phi{<}Z{>}/I \cong \Phi{<}Z{>}_{irr}$. By Lemma 1.3.2 it is clear that V' is a Φ-basis of $\Phi{<}Z{>}_{irr}$ and so V is a Φ-basis for $U(K)$.

Corollary 5.1.2 *Keeping the notations of the proof of Theorem 5.1.1, we set* $ad(\bar{x})(v) = [v, \bar{x}]$ *and* $Ad(\bar{x})(v) = [v^{\phi}, x]^{\psi}$ *for all* $x \in X, v \in L$. *Let* t *be a natural number. Then there exists a sequence* R *of reductions of the form* $R_{A\sigma_{uw}B}$ *such that* $R\left(ad(\bar{x})^t(v)\right) = Ad(\bar{x})^t(v)$.

Proof. Clearly $[\bar{z}, \bar{x}] - [z, x]^{\psi} \in I(\Delta)$ for all $z \in X$. Hence $[u, \bar{x}] - [u^{\phi}, x]^{\psi} \in I(\Delta)$ for all $u \in L$. Therefore

$$ad(\bar{x})(v) - Ad(\bar{x})(v) \in I(\Delta). \tag{5.2}$$

Suppose that

$$ad(\bar{x})^{t-1}(v) - Ad(\bar{x})^{t-1}(v) \in I(\Delta).$$

Then

$$\begin{aligned} &ad(\bar{x})^{t}(v) - ad(\bar{x})\left(ad(\bar{x})^{t-1}(v)\right) \\ &= ad(\bar{x})\left(ad(\bar{x})^{t-1}(v) - Ad(\bar{x})^{t-1}(v)\right) \in I(\Delta). \end{aligned} \tag{5.3}$$

Clearly $Ad(\bar{x})^{t-1}(v) = \left(Ad(x)^{t-1}(v^{\phi})\right)^{\psi} \in L$ for all $t > 0$. By (5.2) it follows that

$$\begin{aligned} &ad(\bar{x})\left(Ad(\bar{x})^{t-1}(v)\right) - Ad(\bar{x})^{t}(v) \\ &= ad(\bar{x})\left(Ad(\bar{x})^{t-1}(v)\right) - Ad(\bar{x})\left(Ad(\bar{x})^{t-1}(v)\right) \in I(\Delta) \end{aligned} \tag{5.4}$$

From (5.3) and (5.4) it follows that

$$ad(\bar{x})^{t}(v) - Ad(\bar{x})^{t}(v) \in I(\Delta).$$

Since $Ad(\bar{x})^{t}(v) \in L \in \Phi{<}Z{>}_{irr}$,

$$\begin{aligned} &N\left(ad(\bar{x})^{t}(v)\right) - Ad(\bar{x})^{t}(v) \\ &= N\left(ad(\bar{x})^{t}(v) - Ad(\bar{x})^{t}(v)\right) \in I(\Delta) \cap \Phi{<}Z{>}_{irr} = 0 \end{aligned}$$

where $N : \Phi{<}Z{>} \rightarrow \Phi{<}Z{>}_{irr}$ is the normal form mapping (its existence follows from Theorem 5.1.1 and the *Diamond Lemma*). Hence $N(ad(\bar{x})^{t}(v)) = Ad(\bar{x})^{t}(v)$. Now our statement follows from the definition of a normal form of an element.

Corollary 5.1.3 *Let $w, u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_n \in \Phi{<}Z{>}$ and $r = \sum_{i=1}^{n} u_i w v_i$. Keeping the notations of the proof of the Theorem 5.1.1, we suppose that there exists a sequence R of reductions of the form $R_{A\sigma_{xy}B}$ such, that $R(w) = 0$. Then there exists a sequence R' of reductions of the same form such that $R'(r) = 0$.*

Proof. Since $R(w) = 0$, $w \in I(\Delta)$. Hence $r \in I(\Delta)$. Clearly $N(r) = 0$. Now our statement follows from the definition of a normal form of an element.

Corollary 5.1.4 *Let K be a Lie algebra over Φ with universal enveloping algebra $(U(K); \rho)$. Assume that K is a free Φ-module. Then $\rho : K \to U(K)^{(-)}$ is a monomorphism of Lie algebras.*

5.2 Restricted Lie Algebras

Let L be a Lie algebra over Φ and $x \in L$. We denote by $ad(x)$ the mapping $L \to L$ given by $ad(x)(y) = [y, x]$. Further let A be an associative ring and $a \in A$. We let r_a and l_a stand for the mappings $A \to A$, given by $r_a(x) = xa$, $l_a(x) = ax$ for all $x \in A$.

Lemma 5.2.1 *Let p be a prime number, Φ the p-element field, X an infinite set, $A = \Phi{<}X{>}$ the free Φ-algebra with 1 generated by X, $L \subseteq A$ the Lie subalgebra generated by X, and $x, y \in X$ Then:*

(a) $ad(x)^p = ad(x^p)$;
(b) $ad(x)^{p-1} = \sum_{i=0}^{p-1} r_x^i l_x^{p-1-i}$, $ad(x)^{p-1} y = \sum_{i=0}^{p-1} x^i y x^{p-1-i}$;
(c) $W(x, y) = (x + y)^p - x^p - y^p \in L$.

Proof. **(a)** Clearly, $r_x l_x = l_x r_x$ and $ad(x) = r_x - l_x$. Since $\binom{p}{i} = \frac{p!}{i!(p-i)!} \equiv 0 \; mod\, p$ for $i \neq 0, p$,

$$ad(x)^p = (r_x - l_x)^p = \sum_i (-1)^i \binom{p}{i} r_x^{p-i} l_x^i = ad(x^p).$$

(b) We show that $\binom{p-1}{i} \equiv (-1)^i \; mod\, p$ for all $i = 0, 1, \ldots, p-1$. We proceed by induction on i. For $i = 0$ this is true. Suppose this is true for $i = k$. Since

$$(-1)^k + \binom{p-1}{k+1} \equiv \binom{p-1}{k} + \binom{p-1}{k+1} = \binom{p}{k+1} \equiv 0 \; mod\, p,$$

$\binom{p-1}{k+1} \equiv (-1)^{k+1}\ mod\ p$ and we are done.

Thus

$$ad(x)^{p-1} = (r_x - l_x)^{p-1} = \sum_i (-1)^i \binom{p-1}{i} r_x^i l_x^{p-1-i} = \sum_i r_x^i l_x^{p-1-i},$$

$$ad(x)^{p-1} y = \sum_{i=0}^{p-1} x^i y x^{p-1-i}.$$

(c) Consider the polynomial ring $A[t]$ and let $\delta : A[t] \to A[t]$ be the derivation given by $t^\delta = 1$ and $a^\delta = 0$ for all $a \in A$.

Note, that the Lie $\Phi[t]$-subalgebra generated by X is equal to $L[t]$. Thus the coefficients of the polynomial $[ad(tx + y)]^{p-1}(x) \in L[t]$ belong to L.

We have:

$$(tx + y)^p = t^p x^p + y^p + \sum_{i=1}^{p-1} t^i s_i(x, y), \tag{5.5}$$

where $s_i(x, y)$ is the coefficient of t^i in the polynomial $(tx + y)^p$. Applying δ to (5.5) one obtains

$$\sum_{i=0}^{p-1} (tx + y)^i x (tx + y)^{p-1-i} = \sum_{i=1}^{p-1} i t^{i-1} s_i(x, y).$$

Taking into account **(b)** we have

$$[ad(tx + y)]^{p-1}(x) = \sum_{i=0}^{p-1} (tx+y)^i x (tx+y)^{p-1-i} = \sum_{i=1}^{p-1} i t^{i-1} s_i(x, y).$$

Thus $i s_i(x, y)$ is the coefficient of t^{i-1} in the polynomial $[ad(tx + y)]^{p-1}(x) \in L[t]$. Hence $s_i(x, y) \in L$. Substituting $t = 1$ into (5.5) we see that $(x + y)^p = x^p + y^p + \sum_{i=1}^{p-1} s_i(x, y)$ and thus $W(x, y) = \sum_{i=1}^{p-1} s_i(x, y) \in L$.

Corollary 5.2.2 *Let A be an associative ring and $pA = 0$ for some prime number p. Then $ad(x)^p = ad(x^p)$ and $(x + y)^p = x^p + y^p + W(x, y)$ for all $x, y \in A$.*

Let p be a prime number and Φ an associative commutative ring with 1 such that $p\Phi = 0$. We recall that a Lie algebra K over Φ with an unary operation $x \mapsto x^{[p]}$ satisfying the identities

$$(\lambda x)^{[p]} = \lambda^p x^{[p]}, \qquad \lambda \in \Phi, x \in K, \tag{5.6}$$

$$ad(x^{[p]}) = ad(x)^p, \qquad x \in K, \tag{5.7}$$

$$(x+y)^{[p]} = x^{[p]} + y^{[p]} + W(x,y), \qquad x, y \in K, \tag{5.8}$$

is said to be *restricted* Lie algebra (or *p-Lie algebra*). Further the operation $x \mapsto x^{[p]}$ is called a *p-operation* .

Note that from Corollary 5.2.2 it follows that the Lie Φ-algebra $A^{(-)}$ with unary operation $x \mapsto x^p$ is restricted.

Let K be a restricted Lie algebra over Φ. A pair $(A; f)$ is said to be a *cover* of the Lie algebra K if A is an associative Φ-algebra with 1 and $f : K \to A^{(-)}$ is a homomorphism of restricted Lie algebras (i.e. $f(x^{[p]}) = f(x)^p$ for all $x \in K$). Notions of enveloping algebra and universal enveloping algebra for restricted Lie algebra are defined analogously to corresponding notions for Lie algebras. The existence of a universal enveloping algebra $(U(K); \phi)$ of a restricted Lie algebra K is proved in the same way as that of a Lie algebra.

Being only interested in restricted Lie algebras which are free Φ-modules, we construct a universal enveloping algebra $(U(K); \rho)$ in much the same fashion as we did for ordinary Lie algebras. The only difference is that we define the ideal $I(K)$ of $\Phi{<}Z{>}$ to be the ideal generated by all elements of the following two forms:

$$\left[u^{\psi}, v^{\psi}\right] - [u,v]^{\psi}, \quad u^{[p]\psi} - \left(u^{\psi}\right)^p, \qquad u, v \in K.$$

Again we leave it for the reader to verify that $(U(K); \rho)$ is indeed a universal enveloping algebra (here $U(K) = \Phi{<}Z{>}/I(K)$ and $\rho = \psi\nu$, where $\psi : K \to L$ and $\nu : \Phi{<}Z{>} \to \Phi{<}Z{>}/I(K)$).

Consider now the ideal I of $\Phi{<}Z{>}$ generated by all elements of the forms:

$$[\bar{x}, \bar{y}] - [x,y]^{\psi}, \quad x^{[p]\psi} - \bar{x}^p, \qquad x, y \in X.$$

We claim that $I(K) = I$. Indeed, the inclusion $I \subseteq I(K)$ is obvious. We denote by μ the projection of $\Phi<Z>$ onto $\Phi<Z>/I$ and set $\tau = \psi\mu$. Since τ is a Φ-linear map and $[x^\tau, y^\tau] = [x,y]^\tau$ for all $x, y \in X$, $[u^\tau, v^\tau] = [u,v]^\tau$ for all $u, v \in K$. Hence τ is a homomorphism of Lie Φ-algebras. It is enough to prove that $(u^\tau)^p = u^{[p]\tau}$ for all $u \in K$ (i.e. τ is a homomorphism of restricted Lie algebras). Let $H = \{u \in K \mid (u^\tau)^p = u^{[p]\tau}\}$. It is clear that $X \subseteq H$. For any $u, v \in H$, $\alpha, \beta \in \Phi$ we have

$$\begin{aligned}
(\alpha u + \beta v)^{[p]\tau} &= \left\{(\alpha u)^{[p]} + (\beta v)^{[p]} + W(\alpha u, \beta v)\right\}^\tau \\
&= \left\{\alpha^p u^{[p]} + \beta^p v^{[p]} + W(\alpha u, \beta v)\right\}^\tau \\
&= \alpha^p u^{[p]\tau} + \beta^p v^{[p]\tau} + W(\alpha u, \beta v)^\tau \\
&= \alpha^p (u^\tau)^p + \beta^p (v^\tau)^p + W(\alpha u, \beta v)^\tau \\
&= \{(\alpha u)^\tau\}^p + \{(\beta v)^\tau\}^p + W(\alpha u, \beta v)^\tau
\end{aligned}$$

Taking into account that $W(x,y)$ is a Lie polynomial in x, y we have

$$\begin{aligned}
(\alpha u + \beta v)^{[p]\tau} &= \{(\alpha u)^\tau\}^p + \{(\beta v)^\tau\}^p + W(\alpha u, \beta v)^\tau \\
&= \{(\alpha u)^\tau\}^p + \{(\beta v)^\tau\}^p + W\left((\alpha u)^\tau, (\beta v)^\tau\right) \\
&= \{(\alpha u)^\tau + (\beta v)^\tau\}^p = \{(\alpha u + \beta v)^\tau\}^p .
\end{aligned}$$

(see Lemma 5.2.1). Hence $\alpha u + \beta v \in H$ and H is a Φ-submodule of K. Since $X \subseteq H$, $H = K$. Thus τ is a homomorphism of restricted Lie algebras and $I = I(K)$.

Theorem 5.2.3 *Let p be a prime number, Φ an associative commutative ring with 1 such that $p\Phi = 0$, K a restricted Lie algebra over Φ and $(U(K); \rho))$ the universal enveloping algebra of the restricted Lie algebra K. Assume that K is a free Φ-module with a well-ordered basis X. Then the set*

$$\begin{aligned}
&V = \{x_1^\rho x_2^\rho \dots x_m^\rho \mid x_j \in X,\ x_1 \le x_2 \le \dots \le x_m \quad \textit{and} \\
&\textit{if} \quad x_k = x_{k+1} = \dots = x_{k+s-1}, \quad \textit{then} \quad s < p\} \cup \{1\}
\end{aligned}$$

is a Φ-basis of $U(K)$ (we shall refer to V as a PBW-basis of the universal enveloping algebra $U(K)$ of the restricted Lie algebra K).

Proof. We continue with the same notations as in Theorem 5.1.1. Consider the reduction system Δ of $\Phi{<}Z{>}$,

$$\begin{aligned} \sigma_{yx} &= \left(\bar{y}\bar{x}, \bar{x}\bar{y} + [y,x]^{\psi}\right) \quad \text{for all} \quad y > x \in X, \\ \sigma_x &= \left(\bar{x}^p, x^{[p]\psi}\right) \quad \text{for all} \quad x \in X. \end{aligned}$$

Let $\leq$ be the linear order on S which was introduced in the proof of Theorem 5.1.1. Clearly this ordering is a semigroup ordering compatible with the reduction system Δ and satisfying the descending chain condition.

It was shown in the proof of Theorem 5.1.1 that for any $P, Q \in S$, $u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_n \in L$ there exists a sequence of reductions R such that

$$R\left(\sum_{i=1}^{n} P[u_i, v_i]Q\right) = \sum_{i=1}^{n} P\left[u_i^{\phi}, v_i^{\phi}\right]^{\psi} Q. \tag{5.9}$$

Let $I = I(\Delta)$ be the ideal of the algebra A generated by the reduction system Δ. It is clear that the ideal I is generated by all elements of the form $[\bar{x}, \bar{y}] - [x, y]^{\psi}$ and $\bar{x}^p - x^{[p]\psi}$, $x, y \in X$.

We will show that all ambiguities of Δ are resolvable and the set

$$\begin{aligned} V' = \quad & \{\bar{x}_1\bar{x}_2\ldots\bar{x}_m \mid x_i \in X \; x_1 \leq x_2 \leq \ldots \leq x_m \quad \text{and} \\ & \text{if} \quad x_k = x_{k+1} = \ldots = x_{k+s-1}, \quad \text{then} \quad s < p\} \cup \{1\} \end{aligned}$$

is a Φ-basis of $\Phi{<}Z{>}_{irr}$.

Indeed, let us consider the various ambiguities.

Case 1. Overlap ambiguity $(\sigma_{zy}, \sigma_{yx}, \bar{z}, \bar{y}, \bar{x})$, where $x, y, z \in X$ and $z > y > x$. It was shown in the proof of Theorem 5.1.1 that this ambiguity is resolvable.

Case 2. Overlap ambiguity $(\sigma_{yx}, \sigma_x, \bar{y}, \bar{x}, \bar{x}^{p-1})$, where $x, y \in X$ and $y > x$.We set

$$\begin{aligned} w &= R_{y\sigma_x}\left(\bar{y}\bar{x}^p\right) - R_{\sigma_{yx}x^{p-1}}\left(\bar{y}\bar{x}^p\right) \\ &= \bar{y}x^{[p]\psi} - \left(\bar{x}\bar{y} + [y,x]^\psi\right)\bar{x}^{p-1}, \\ w' &= R_{x^{p-1}\sigma_{yx}} \dots R_{x^2\sigma_{yx}x^{p-3}} R_{x\sigma_{yx}x^{p-2}}(w) \\ &= \bar{y}x^{[p]\psi} - \bar{x}^p\bar{y} - \sum_{i=0}^{p-1} \bar{x}^i[y,x]^\psi \bar{x}^{p-1-i}, \end{aligned}$$

and

$$w'' = R_{\sigma_x y}(w') = \bar{y}x^{[p]\psi} - x^{[p]\psi}\bar{y} - \sum_{i=0}^{p-1} \bar{x}^i[y,x]^\psi\bar{x}^{p-1-i}.$$

Assume that $p = 2$. Then

$$w'' = [\bar{y}, x^{[2]\psi}] - [y,x]^\psi\bar{x} - \bar{x}[y,x]^\psi = [\bar{y}, x^{[2]\psi}] - \left[[y,x]^\psi, \bar{x}\right].$$

By (5.9) we may reduce this element to

$$[y, x^{[2]}]^\psi - [[y,x],x]^\psi = 0,$$

since K is a restricted Lie algebra.

We consider now the case $p > 2$. Then the length of any monomial in $\bar{y}x^{[p]\psi} - x^{[p]\psi}\bar{y}$ is equal to 2 while the length of any monomial in $\sum_{i=0}^{p-1}\bar{x}^i[y,x]^\psi\bar{x}^{p-1-i}$ is equal to $p > 2$. Obviously, we may reduce the element $[\bar{y}, x^{[p]\psi}]$ to $[y, x^{[p]}]^\psi$, such that the element $\sum_{i=0}^{p-1}\bar{x}^i[y,x]^\psi\bar{x}^{p-1-i}$ will not change. By Lemma 5.2.1 it follows that

$$\sum_{i=0}^{p-1}\bar{x}^i[y,x]^\psi\bar{x}^{p-1-i} = ad(\bar{x})^{p-1}\left([y,x]^\psi\right).$$

Taking into account Corollary 5.1.2 we find that this element may be reduced to

$$\begin{aligned} Ad(\bar{x})^{p-1}\left([y,x]^\psi\right) &= \left\{ad(x)^{p-1}\left([y,x]\right)\right\}^\psi \\ &= \{ad(x)^p(y)]\}^\psi = [y, x^{[p]}]^\psi. \end{aligned}$$

Thus, the element w'' (and, therefore, the element w) may be reduced to 0 and this ambiguity is resolvable.

Case 3. Overlap ambiguity $(\sigma_x, \sigma_{xy}, \bar{x}^{p-1}, \bar{x}, \bar{y})$, where $x, y \in X$ and $x > y$. This case is considered by analogy with case 2.

Case 4. Overlap ambiguity $(\sigma_x, \sigma_x, \bar{x}^l, \bar{x}^{p-l}, \bar{x}^l)$, where $x \in X$. We set

$$\begin{aligned} w &= R_{\sigma_x x^l}\left(\bar{x}^{p+l}\right) - R_{x^l \sigma_x}\left(\bar{x}^{p+l}\right) = x^{[p]\psi}\bar{x}^l - \bar{x}^l x^{[p]\psi} \\ &= \left[x^{[p]\psi}, \bar{x}^l\right] = \sum_{i=0}^{l-1} \bar{x}^i \left[x^{[p]\psi}, \bar{x}\right] \bar{x}^{l-i-1}. \end{aligned}$$

By (5.9) it follows that $R\left(\left[x^{[p]\psi}, \bar{x}\right]\right) = \left[x^{[p]}, x\right]^{\psi}$ for some sequence R of reductions of the form $R_{A\sigma_{yz}B}$. Since K is a restricted Lie algebra,

$$\left[x^{[p]}, x\right] = ad(x)^p(x) = ad(x)^{p-1}\left(ad(x)(x)\right) = 0.$$

Taking into account Corollary 5.1.3 we find that the element w may be reduced to 0. Thus this ambiguity is resolvable.

With all ambiguities resolved, we can now assert (just as in the proof of Theorem 5.1.1) that the Diamond Lemma together with Lemma 1.3.2 imply that V is a Φ-basis for $U(K)$.

Corollary 5.2.4 *Let K be a restricted Lie algebra over Φ with universal enveloping algebra $(U(K), \rho)$. Assume that K is a free Φ-module. Then $\rho : K \to U(K)^{(-)}$ is a monomorphism of restricted Lie algebras.*

5.3 Differential Lie Algebras

Let Φ be an associative commutative ring with an identity element e and $F \supseteq \Phi$ an associative commutative Φ-algebra with same identity e. Furthermore let A be a Φ-algebra with 1 which is also an F-ring.

Slightly generalizing the definition of a differential Lie algebra (see Baer [14], Jacobson [131], Kharchenko [146] and [147]) we make the following

Definition 5.3.1 *A subset $L \subseteq A$ is said to be a special differential F-Lie algebra over Φ (SDL-algebra) with cover algebra A, if the following conditions hold:*

(a) $[a, b] \in L$ for all $a, b \in L$;

(b) $a\lambda + b\mu \in L$ for all $a, b \in L$, $\lambda, \mu \in F$;

(c) $[1 \cdot \lambda, a] \in 1 \cdot F$ for all $a \in L$, $\lambda \in F$;

(d) $Ann_F(L) = Ann_F(A)$ (i.e., $L\lambda = 0$ implies $1 \cdot \lambda = 0$ for all $\lambda \in F$).

Let I be an ideal of the Φ-algebra F. We denote by $Der(F/I)$ the set of all derivations of the factor algebra F/I. One may verify that $Der(F/I)$ with multiplication $[\delta_1, \delta_2] = \delta_1\delta_2 - \delta_2\delta_1$ is a Lie Φ-algebra. Further let $\delta \in Der(F/I)$, $c \in F$. We set $x^{\delta c} = x^{\delta}c$ for all $x \in F/I$. Clearly δc is a derivation of F/I. Thus $Der(F/I)$ is a right F-module. Analogously $Der(F/I)$ is a right F/I-module.

Definition 5.3.2 *A triple $(K; F; \Lambda)$ is said to be a differential F-Lie algebra (DL-algebra), if the following conditions hold:*

(a) K is a Lie Φ-algebra;

(b) K is a right F-module;

(c) $\Lambda : K \to Der(F/Ann_F(K)$ is a homomorphism of Lie Φ-algebras, which is also a homomorphism of right F-modules;

(d) $[\delta c, \mu] = [\delta, \mu]c + \delta c^{\hat{\mu}}$ (where $\hat{\mu} = \Lambda(\mu)$) for all $\delta, \mu \in K$, $c \in F$.

In what follows $\hat{\mu} = \Lambda(\mu)$ for a DL-algebra K. Let $L \subseteq A$ be an SDL-algebra. Note that $F/Ann_F(L) \cong 1 \cdot F$ under the mapping $c + Ann_F(L) \mapsto 1 \cdot c$ for all $c \in F$. Define the mapping $\Lambda : L \to Der(1 \cdot F)$, setting $(1 \cdot c)^{\Lambda(a)} = [1 \cdot c, a]$ for all $c \in F$, $a \in$

L. It immediately follows from Definition 5.3.1 that $(L; F; \Lambda)$ is a DL-algebra.

We remark that in case F is a field some obvious simplifications occur. Part **(d)** of Definition 5.3.1 may be omitted, and the ideal $Ann_F(K) = 0$ wherever it appears (i.e., in Definitions 5.3.2 and 5.3.9 and Proposition 5.3.10).

Definition 5.3.3 *Let K, L be DL-algebras. Then a mapping $f : K \to L$ is said to be a homomorphism of DL-algebras, if the following conditions hold:*

(a) f is a homomorphism of Lie Φ-algebras;

(b) f is a homomorphism of right F-modules;

(c) $\widehat{\delta^f} = \hat{\delta}$ for all $\delta \in K$.

Definition 5.3.4 *Let K be a differential F-Lie algebra. A pair $((A; L); f)$ is said to be a cover of the DL-algebra K, if $L \subseteq A$ is a special differential F-Lie algebra with the cover A and $f : K \to L$ is a homomorphism of DL-algebras. A cover $((A; L); f)$ of the DL-algebra K is called an enveloping algebra of K if $A = \langle K^f \rangle + 1 \cdot F$, where $\langle K^f \rangle$ is the subalgebra of A generated by the set K^f. Two covers $((A; L); f)$ and $((B; M); g)$ of a DL-algebra K are said to be isomorphic if there exists an isomorphism $h : A \to B$ of F-rings such that $fh = g$. An enveloping algebra $((U; M); \phi)$ of the DL-algebra K is said to be a universal enveloping algebra of K if for any cover algebra $((A; L); f)$ of K there exists a (necessarily unique) homomorphism of F-rings $\psi : U \to A$ such that $\phi\psi = f$.*

It would perhaps be more realistic to refer to a cover algebra as a cover ring (since F rather than Φ is the important ring of scalars) and accordingly use the term universal enveloping ring. However, we shall keep the (more customary) terms of cover algebra and universal enveloping algebra.

Clearly, a universal enveloping algebra of a given DL-algebra, if it exists, is determined uniquely up to isomorphism. We shall presently construct the universal enveloping algebra of K.

Lemma 5.3.5 *Let $(K; F; \Lambda)$ be a differential F-Lie algebra and let $K' = K \oplus F$ be the direct sum of right F-modules. We set*

$$[x+f, y+g] = [x,y] + f^{\hat{y}} - g^{\hat{x}} \quad \textit{for all} \quad x, y \in K, \ f, g \in F.$$

Define the mapping $\Lambda' : K' \to Der(F)$, setting $\Lambda'(x+f) = \Lambda(x)$ for all $x \in K$, $f \in F$. Then $(K'; F; \Lambda')$ is a differential F-Lie algebra.

Proof. First of all we show that K' is a Lie Φ-algebra. Clearly $[x+f, x+f] = 0$ for all $x \in K$, $f \in F$. It is enough to prove that the Jacobi identity holds in K'. For all $x, y, z \in K$, $f, g, h \in F$ we have

$$\begin{aligned}
&[x+f,[y+g,z+h]] + [z+h,[y+g,x+f]] \\
&+ [y+g,[x+f,z+h]] = \left[x+f,[y,z]+g^{\hat{z}}-h^{\hat{y}}\right] \\
&+ \left[z+h,[x,y]+f^{\hat{y}}-g^{\hat{x}}\right] + \left[y+g,[z,x]+h^{\hat{x}}-f^{\hat{z}}\right] \\
&= [x,[y,z]] + f^{\Lambda([y,z])} - g^{\hat{z}\hat{x}} + h^{\hat{y}\hat{x}} \\
&+ [z,[x,y]] + h^{\Lambda([x,y])} - f^{\hat{y}\hat{z}} + g^{\hat{x}\hat{z}} \\
&+ [y,[z,x]]] + g^{\Lambda([z,x])} - h^{\hat{x}\hat{y}} + f^{\hat{z}\hat{y}} \\
&= f^{\Lambda([y,z])} - \left(f^{\hat{y}\hat{z}} - f^{\hat{z}\hat{y}}\right) + g^{\Lambda([z,x])} - \left(g^{\hat{z}\hat{x}} - g^{\hat{x}\hat{z}}\right) \\
&+h^{\Lambda([x,y])} - \left(h^{\hat{x}\hat{y}} - h^{\hat{y}\hat{x}}\right) = 0,
\end{aligned}$$

since the Jacobi identity holds in K and Λ is a homomorphism of Lie algebras.

Clearly Λ' is a homomorphism of Lie Φ-algebras. Further

$$\begin{aligned}
[(x+f)c, y+g] &= [xc+fc, y+g] = [xc,y] + (fc)^{\hat{y}} - g^{\Lambda(xc)} \\
&= [x,y]c + xc^{\hat{y}} + f^{\hat{y}}c + fc^{\hat{y}} - g^{\hat{x}c} \\
&= [x,y]c + xc^{\hat{y}} + f^{\hat{y}}c + fc^{\hat{y}} - g^{\hat{x}}c \\
&= \left([x,y] + f^{\hat{y}} - g^{\hat{x}}\right)c + (x+f)c^{\hat{y}} \\
&= [x+f, y+g]c + (x+f)c^{\Lambda'(y+g)}
\end{aligned}$$

for all $x, y \in K$, $f, g, c \in F$. Thus all the conditions of Definition 5.3.2 hold in K' and K' is a differential F-Lie algebra.

Before proving the main theorem of this section, we make the following observations. Assume that K is a free right F-module with a basis X, F is a free Φ-module with a basis G and the identity element e of the ring F belongs to G. Now we proceed to describe the universal enveloping algebra $U(K)$ as a factor algebra of a free Φ-algebra. Clearly $G \cup \{xg \mid x \in X,\ g \in G\}$ is a basis of the Φ-module $K' = K \oplus F$. Let $Z = \{\bar{x} \mid x \in X\} \cup \{\bar{g} \mid g \in G\}$, $S = S{<}Z{>}$ the free semigroup (with 1), and $\Phi{<}Z{>}$ the free Φ-algebra (with 1) generated by the set Z. Denote by L the Φ-span of $\{\bar{g} \mid g \in G\} \cup \{\bar{x}\bar{g} \mid x \in X,\ g \in G\}$ in $\Phi{<}Z{>}$ and let $\psi : K' \to L$ be the Φ-map given by $g \mapsto \bar{g}$, $xg \mapsto \bar{x}\bar{g}$ for all $g \in G$, $x \in X$. Obviously ψ is an isomorphism of Φ-modules and we set $\phi = \psi^{-1}$. We define $I(K)$ to be the ideal of $\Phi{<}Z{>}$ generated by $\bar{e} - 1$ and all elements of the form $(ua)^\psi - u^\psi a^\psi$, $[u, v]^\psi - [u^\psi, v^\psi]$ for all $a \in F$, $u, v \in K'$, or, equivalently, $\bar{e} - 1$, $(ba)^\psi - \bar{b}\bar{a}$, $[x, y]^\psi - [\bar{x}, \bar{y}]$, $[a, x]^\psi - \left(a^{\hat{x}}\right)^\psi$ for all $a, b \in G$, $x, y \in X$. Letting ν denote the projection of $\Phi < Z >$ onto $U = U(K) = \Phi < Z > /I(K)$, we set $\rho = \psi\nu$ and $M = L^\nu = K'^\rho$. Note that $(ua)^\rho = u^\rho a^\rho$, $[u, v]^\rho - [u^\rho, v^\rho]$ for all $a \in F$, $u, v \in K'$. Hence $MF^\rho = M$ and $[M, M] \subseteq M$. Moreover ρ is a homomorphism of Lie algebras over Φ. Recalling that $F \subseteq K'$ and $\bar{e} - 1 \in I(K)$, we infer that $F^\rho F^\rho = F^\rho$ and $1 \in F^\rho$. Therefore F^ρ is a subalgebra of the Φ-algebra U. Clearly ρ induces a homomorphism $F \to F^\rho$ of Φ-algebras. Thus the algebra U is a right F-module under the operation $u \cdot a = ua^\rho$ for all $u \in U$, $a \in F$. It immediately follows from the above that M is a submodule of the right F-module U and ρ is a homomorphism of right F-modules. Further

$$[1 \cdot c, u^\rho] = [c^\rho, u^\rho] = [c, u]^\rho = c^{\hat{u}\rho} = 1 \cdot c^{\hat{u}} \in 1 \cdot F$$

for all $c \in F$, $u \in K'$. Hence M is a special differential F-Lie algebra over Φ. The reader may now verify the straightforward details that ρ is a homomorphism of DL-algebras.

Let $((A;N);f)$ be any cover of the DL-algebra K. Define the mapping $f' : K' \to N + 1 \cdot F$, setting $(k+c)^{f'} = k^f + 1 \cdot c$ for all $k \in K$, $c \in F$. It easily follows from the definitions that $((A;N);f')$ is a cover of the DL-algebra K'. Lifting f' to a homomorphism $\sigma : \Phi < Z > \to A$ and recalling that f' is a homomorphism of right F-modules and Lie algebras over Φ, we see that $I(K)^{f'} = 0$. Thus $(U(K);\rho)$ is the universal enveloping algebra of K', whence, with ρ restricted to K, $((U;\ M);\ \rho)$ is also the universal enveloping algebra $(U;\rho)$ of K.

Now we are ready to prove the main theorem of this section.

Theorem 5.3.6 *Let $(K;F;\Lambda)$ be a DL-algebra with the universal enveloping algebra $(U(K);\rho)$, assuming that F is a free Φ-module and K is a free right F-module with a well-ordered ordered basis X. Then the set*

$$V = \{x_1^\rho x_2^\rho \ldots x_m^\rho \mid x_j \in X,\ x_1 \le x_2 \le \ldots \le x_m\} \cup \{1\}$$

is a basis of the right F-module $U(K)$ (we shall refer to V as a PBW-basis of the universal enveloping algebra $U(K)$ of the DL-algebra K).

Proof. Without loss of generality we may assume that G is well-ordered. Define a well-ordering on the set $Z = \{\bar{x} \mid x \in X\} \cup \{\bar{g} \mid g \in G\}$, setting $\bar{u} < \bar{v}$ if either $u, v \in X$ and $u < v$, or $u, v \in G$ and $u < v$, or $u \in X$ and $v \in G$, for all $\bar{u}, \bar{v} \in Z$.

We continue with the same notations as in Theorem 5.1.1. Consider the reduction system Δ of Φ<Z>,

$$\begin{aligned}
\sigma_{yx} &= \left(\bar{y}\bar{x}, \bar{x}\bar{y} + [y,x]^\psi\right), \quad \text{for all} \quad y > x \in X;\\
\chi_{gx} &= \left(\bar{g}\bar{x}, \bar{x}\bar{g} + \left(g^{\hat{x}}\right)^\psi\right), \quad \text{for all} \quad g \in G,\ x \in X;\\
\omega_{gq} &= \left(\bar{g}\bar{q}, (gq)^\psi\right), \quad \text{for all} \quad g, q \in G;\\
\pi_e &= (\bar{e}, 1).
\end{aligned}$$

Let $\leq$ be the linear order on S which was introduced in the proof of Theorem 5.1.1. Clearly this ordering is a semigroup ordering compatible with the reduction system Δ and satisfying the descending chain condition. Further, let $I = I(\Delta)$ be the ideal of the algebra $\Phi<Z>$ generated by the reduction system Δ. We note that $I(K) = I(\Delta)$ and so $U(K) = \Phi<Z>/I(\Delta)$.

Now let $c \in F$ and $x \in X$. We claim that there exists a sequence R of reductions of the form $R_{\chi_{gx}}$ such that

$$R(c^{\psi}\bar{x}) = \bar{x}c^{\psi} + \left(c^{\hat{x}}\right)^{\psi}.$$

Indeed, let $c = \sum_{i=1}^{n} \alpha_i g_i$, where $\alpha_i \in \Phi$. We set

$$R = R_{\chi_{g_1 x}} R_{\chi_{g_2 x}} \dots R_{\chi_{g_n x}}.$$

Then

$$\begin{aligned} R(c^{\psi}\bar{x}) &= R(\sum_i \alpha_i \bar{g}_i \bar{x}) = \sum_i \alpha_i R(\bar{g}_i \bar{x}) \\ &= \sum_i \alpha_i \bar{x} \bar{g}_i + \sum_i \alpha_i \left(g_i^{\hat{x}}\right)^{\psi} \\ &= \bar{x}c^{\psi} + \left(c^{\hat{x}}\right)^{\psi}. \end{aligned}$$

Analogously one may prove the following statements. For any $c \in F$ and $u \in K$ there exists a sequence R of reductions of the form $R_{\chi_{gx}}$ such that

$$R(c^{\psi}u^{\psi}) = u^{\psi}c^{\psi} + \left(c^{\hat{u}}\right)^{\psi}. \tag{5.10}$$

Further for all $c \in F$ and $x, y \in X$ there exists a sequence R of reductions of the form

$$R_{\chi_{gxy}}, R_{\chi_{gy}}, \quad \text{and} \quad R_{x\chi_{gy}}$$

such that

$$R(c^{\psi}\bar{x}\bar{y}) = \bar{x}\bar{y}c^{\psi} + \bar{x}\left(c^{\hat{y}}\right)^{\psi} + \bar{y}\left(c^{\hat{x}}\right)^{\psi} + \left(c^{\hat{x}\hat{y}}\right)^{\psi}. \tag{5.11}$$

Moreover for all $c \in F$ and $x, y \in X$ there exists a sequence R of reductions of the form $R_{y\chi_{gx}}$ such that

$$R(\bar{y}c^{\psi}\bar{x}) = \bar{y}\bar{x}c^{\psi} + \bar{y}\left(c^{\hat{x}}\right)^{\psi}. \tag{5.12}$$

Now let $a, b \in F$ and $x \in X$. In a similar fashion one may show that

$$R(a^{\psi}b^{\psi}) = (ab)^{\psi},\ R'(a^{\psi}b^{\psi}\bar{x}) = \bar{x}(ab)^{\psi} + \left((ab)^{\hat{x}}\right)^{\psi} \tag{5.13}$$

for some sequences R and R' of reductions of the forms $R_{\omega_{gh}}$ and $R_{\omega_{gh}x}$, $R_{\chi_{gx}}$ respectively.

We show that all ambiguities of Δ are resolvable and the set

$$V' = \{\bar{x}_1\bar{x}_2\ldots\bar{x}_m\bar{g} \mid x_j \in X,\ g \in G,\ x_1 \leq x_2 \leq \ldots \leq x_m\} \cup \bar{G}$$

is a Φ-basis of $\Phi{<}Z{>}_{irr}$.

Indeed, let us consider the various ambiguities.

Case 1. Overlap ambiguity $(\sigma_{zy}, \sigma_{yx}, \bar{z}, \bar{y}, \bar{x})$, where $x, y, z \in X$ and $z > y > x$. It was shown in the proof of Theorem 5.1.1 that this ambiguity is resolvable.

Case 2. Overlap ambiguity $(\chi_{gy}, \sigma_{yx}, \bar{g}, \bar{y}, \bar{x})$, where $x, y \in X$, $g \in G$ and $y > x$. We set

$$\begin{aligned} u &= R_{g\sigma_{yx}}(\bar{g}\bar{y}\bar{x}) = \bar{g}[y,x]^{\psi} + \bar{g}\bar{x}\bar{y}, \\ v &= R_{\chi_{gy}x}(\bar{g}\bar{y}\bar{x}) = \bar{y}\bar{g}\bar{x} + \left(g^{\hat{y}}\right)^{\psi}\bar{x}. \end{aligned}$$

Since $R_{\chi_{gz}}(\bar{g}\bar{x}\bar{y}) = \bar{g}\bar{x}\bar{y}$ for all $z \in X$, from (5.10) it follows that there exists a sequence R_1 of reductions such that

$$R_1(u) = [y,x]^{\psi}\bar{g} + \left(g^{\widehat{[y,x]}}\right)^{\psi} + \bar{g}\bar{x}\bar{y}.$$

As $\left(g^{\widehat{[y,x]}}\right)^{\psi} = \left(g^{\hat{y}\hat{x}}\right)^{\psi} - \left(g^{\hat{x}\hat{y}}\right)^{\psi}$, we infer from (5.11) that

$$\begin{aligned} & R_2R_1(u) \\ = \ & [y,x]^{\psi}\bar{g} + \left(g^{\widehat{[y,x]}}\right)^{\psi} + \bar{x}\bar{y}\bar{g} + \bar{x}\left(g^{\hat{y}}\right)^{\psi} + \bar{y}\left(g^{\hat{x}}\right)^{\psi} + \left(g^{\hat{x}\hat{y}}\right)^{\psi} \\ = \ & [y,x]^{\psi}\bar{g} + \bar{x}\bar{y}\bar{g} + \bar{x}\left(g^{\hat{y}}\right)^{\psi} + \bar{y}\left(g^{\hat{x}}\right)^{\psi} + \left(g^{\hat{y}\hat{x}}\right)^{\psi} \end{aligned} \tag{5.14}$$

for some reduction sequence R_2. From (5.10) it follows that

$$R_3(v) = \bar{y}\bar{g}\bar{x} + \bar{x}\left(g^{\hat{y}}\right)^{\psi} + \left(g^{\hat{y}\hat{x}}\right)^{\psi}$$

for some reduction sequence R_3. Using (5.12) we obtain

$$R_4R_3(v) = \bar{y}\bar{x}\bar{g} + \bar{y}\left(g^{\hat{x}}\right)^{\psi} + \bar{x}\left(g^{\hat{y}}\right)^{\psi} + \left(g^{\hat{y}\hat{x}}\right)^{\psi}$$

for some reduction sequence R_4. Now we have

$$R_{\sigma_{yxg}}R_4R_3(v) = [y,x]^{\psi}\bar{g} + \bar{x}\bar{y}\bar{g} + \bar{y}\left(g^{\hat{x}}\right)^{\psi} + \bar{x}\left(g^{\hat{y}}\right)^{\psi} + \left(g^{\hat{y}\hat{x}}\right)^{\psi}.$$

Comparing with (5.14) we conclude that this ambiguity is resolvable.

Case 3. Overlap ambiguity $(\omega_{hg}, \sigma_{gx}, \bar{h}, \bar{g}, \bar{x})$, where $x \in X$, $g, h \in G$. We set

$$\begin{aligned} u &= R_{h\chi_{gx}}(\bar{h}\bar{g}\bar{x}) = \bar{h}\bar{x}\bar{g} + \bar{h}\left(g^{\hat{x}}\right)^{\psi}, \\ v &= R_{\omega_{hg}x}(\bar{h}\bar{g}\bar{x}) = (hg)^{\psi}\bar{x}. \end{aligned}$$

From (5.13) we infer that $R_1(u) = \bar{h}\bar{x}\bar{g} + \left(hg^{\hat{x}}\right)^{\psi}$ for some reduction sequence R_1. Clearly $R_{\chi_{hxg}}R_1(u) = \bar{x}\bar{h}\bar{g} + \left(h^{\hat{x}}\right)^{\psi}\bar{g} + \left(hg^{\hat{x}}\right)^{\psi}$. Again by (5.13) we have that

$$\begin{aligned} R_2R_{\chi_{hxg}}R_1(u) &= \bar{x}\bar{h}\bar{g} + \left(h^{\hat{x}}g\right)^{\psi} + \left(hg^{\hat{x}}\right)^{\psi} \\ &= \bar{x}\bar{h}\bar{g} + \left(h^{\hat{x}}g + hg^{\hat{x}}\right)^{\psi} \\ &= \bar{x}\bar{h}\bar{g} + \left((hg)^{\hat{x}}\right)^{\psi} \end{aligned}$$

for some reduction sequence R_2. Now we have

$$\begin{aligned} R_{x\omega_{hg}}R_2R_{\chi_{hxg}}R_1(u) &= \bar{x}(hg)^{\psi} + \left((hg)^{\hat{x}}\right)^{\psi} \\ &= R_3(v) \end{aligned}$$

for some reduction sequence R_3 (see (5.10)). Therefore this ambiguity is resolvable also.

Case 4. Inclusion ambiguity $(\pi_e, \chi_{ex}, \bar{e}, \bar{x})$, where $x \in X$. Since e is the identity of F, $e^{\hat{x}} = (e^2)^{\hat{x}} = ee^{\hat{x}} + e^{\hat{x}}e = 2e^{\hat{x}}$ and $e^{\hat{x}} = 0$. So $R_{x\pi_e}R_{\chi_{ex}}(\bar{e}\bar{x}) = x = R_{\pi_e x}(x)$ and this ambiguity is resolvable.

Case 5. Overlap ambiguity $(\omega_{gp}, \omega_{pq}, \bar{g}, \bar{p}, \bar{q})$, where $g, p, q \in G$. It easily follows from (5.13) that this ambiguity is resolvable.

Case 6. Inclusion ambiguity $(\pi_e, \omega_{eg}, \bar{e}, \bar{g})$, where $g \in G$. Since $R_{\pi_e g}(\bar{e}\bar{g}) = \bar{g} = (eg)^{\psi} = R_{\omega_{eg}}(\bar{e}\bar{g})$, this ambiguity is resolvable.

Case 7. Inclusion ambiguity $(\omega_{ge}, \pi_e, \bar{g}, \bar{e})$, where $g \in G$. Obviously it is resolvable.

Again we are in the situation where the Diamond Lemma and Lemma 1.3.2 imply that V' is a Φ-basis for $U(K)$. It follows immediately that V is a right F-module basis of $U(K)$ and the proof is complete.

Corollary 5.3.7 *Let $(K; F; \Lambda)$ be a DL-algebra with the universal enveloping algebra $(U(K); \phi)$. Assume that F is a free Φ-module, and K is a free right F-module. Then $\rho : K \to U(K)^{(-)}$ is a monomorphism of differential Lie algebras.*

In section 5.4 we will need the following (we keep the notations of the proof of Theorem 5.3.6)

Lemma 5.3.8 *Suppose that $p\Phi = 0$ for some prime number p. Let $g \in G$ and $x \in X$. Then there exists a sequence R of reductions of the form*

$$R_{A\sigma_{yz}B},\ R_{A\chi_{hy}B},\ R_{A\omega_{ht}B},\ R_{A\pi_e B}$$

such that $R\left(\bar{x}\bar{g}\bar{x}^{p-1} + g^{\hat{x}\psi}\bar{x}^{p-1}\right) = \bar{x}^p\bar{g} + Ad(\bar{x})^p(\bar{g})$.

Proof. Let $u = \bar{g}\bar{x}^p$ and $v = \bar{x}\bar{g}\bar{x}^{p-1} + g^{\hat{x}\psi}\bar{x}^{p-1}$. Since $R_{\chi_{gx}x^{p-1}}(u) = v$, $u - v \in I(K)$. By Lemma 5.2.1, $ad(\bar{x})^p(\bar{g}) = \bar{g}\bar{x}^p - \bar{x}^p\bar{g}$. Now it follows from Corollary 5.1.2 that $\bar{g}\bar{x}^p - \bar{x}^p\bar{g} - Ad(\bar{x})^p(\bar{g}) \in I(K)$. Thus the element u is reducible to the element $\bar{x}^p\bar{g} + Ad(\bar{x})^p(\bar{g}) \in \Phi{<}Z{>}_{irr}$. Since $u - v \in I(K)$, they have the same normal form and we are done.

In order to discuss some useful properties of universal enveloping algebras, we need the following notion.

Definition 5.3.9 *Let K, L be differential Lie algebras and let $\tau : F/Ann_F(K) \to F/Ann_F L$ be an isomorphism of Φ-algebras. Then a mapping $f : K \to L$ is said to be a τ-semilinear homomorphism of DL-algebras, if the following conditions hold:*
(a) f is a homomorphism of Lie Φ-algebras;
(b) $(\delta c)^f = \delta^f c^\tau$ for all $\delta \in K$, $c \in F/Ann_F(K)$;
(c) $\widehat{\delta^f} = \tau^{-1}\hat{\delta}\tau$ for all $\delta \in K$.

Proposition 5.3.10 *Let $(K; F; \Lambda)$ be a DL-algebra, $(U(K); \rho)$ the universal enveloping algebra of K, $L \subseteq A$ a special differential F-Lie algebra over Φ and $h : K \to L$ a τ-semilinear homomorphism of DL-algebras. Then there is a unique homomorphism $h' : U(K) \to A$ of Φ-algebras such that $\rho h' = h$ and $h'(uc) = h'(u)(c + Ann_F(K))^\tau$ for all $u \in U(K)$, $c \in F$.*

Proof. According to Definition 5.3.1, $Ann_F(L) = Ann_F(A)$. We consider A and L as Φ-algebras A^* and L^* respectively with right F-module structures given by the rule $a \circ c = a(c + Ann_F(K))^\tau$, $l \circ c = l(c + Ann_F(K))^\tau$ for all $a \in A$. $l \in L$, $c \in F$. Clearly L^* is a submodule of the right F-module A^*. Further

$$[1 \circ c, l] = [1 \cdot (c + Ann_F(K))^\tau, l] \in 1 \cdot F = 1 \circ F.$$

Hence $L^* \subseteq A^*$ is an SDL-algebra. The reader may now verify the straightforward details that h is a homomorphism of DL-algebras. By the definition of a universal enveloping algebra of a

DL-algebra, it follows that there exists a unique homomorphism $h' : U(K) \to A$ of F-rings with identity such that $\rho h' = h$. Since $h'(uc) = h'(u) \circ c = h'(u)(c + Ann_F(K))^\tau$, we are done.

Corollary 5.3.11 *Let $(K; F; \Lambda)$ be a DL-algebra with the universal enveloping algebra $(U(K); \phi)$. Then for any τ-semilinear automorphism $h : K \to K$ of DL-algebras there exists a unique τ-semilinear automorphism $h' : U(K) \to U(K)$ of Φ-algebras such that $\rho h' = h\rho$.*

Proof. We apply Proposition 5.3.10 to h and h^{-1}.

5.4 Restricted Differential Lie Algebras

Let p be a prime number, Φ a commutative ring with identity element e such that $p\Phi = 0$ and $F \supseteq \Phi$ a commutative Φ-algebra with same identity. Furthermore let A be a Φ-algebra with 1 which is also an F-ring.

Definition 5.4.1 *A subset $L \subseteq A$ is said to be a special restricted differential F-Lie algebra over Φ (p-SDL-algebra) with the cover algebra A, if L is an SDL-algebra and $a^p \in L$ for all $a \in L$.*

As motivation for the definition of an abstract restricted differential F-Lie algebra we have the following lemma.

Lemma 5.4.2 *Let $L \subseteq A$ be a p-SDL algebra, $H = 1 \cdot F$ and $a \in L$. Define mappings $T_{n,a} : H \to H$, $n = 1, 2, \dots, p$, setting*

$$T_{1,a}(c) = c, \quad T_{n+1,a}(c) = [T_{n,a}(c), a]\, c$$

for all $c \in H$. Then:

(a) $(ad(a)|_H c)^p = (ad(a)|_H)^p\, c^p + (ad(a)|_H)\, T_{p,a}(c)$;
(b) $(ac)^p = a^p c^p + aT_{p,a}(c)$;
(c) $(a + c)^p = a^p + c^p + ad(a)^{p-1}(c)$.

Proof. **(a)** Letting μ denote the mapping $ad(a)|_H$, we note that μ is a derivation of the Φ-algebra H (recall that $[H,a] \subseteq H$). Setting $T_{n,\mu}(c) = T_{n,a}(c)$, we observe that

$$T_{1,\mu}(c) = c, \quad T_{n+1,\mu}(c) = (T_{n,\mu}(c))^{\mu} c.$$

Let R be a commutative ring such that $pR = 0$, $x \in R$, and let $\delta : R \to R$ be a derivation. Recall that $x^{\mu r} = x^{\mu} r$ for all $r \in R$. One may prove the following formula by an obvious induction on n:

$$x^{(\delta r)^n} = x^{\delta^n} r^n + \sum_{i=2}^{n-1} x^{\delta^i} P_{n,i,\delta}(r) + x^{\delta} T_{n,\delta}(r), \tag{5.15}$$

where $P_{n,i,\delta}(r)$ is a polynomial in $r, r^{\delta}, \ldots, r^{\delta^{n-i}}$ with integral coefficients. We claim that $P_{p,i,\delta}(r) = 0$ for all $i = 2, 3, \ldots, p-1$.

Indeed, consider the polynomial ring $K = \Phi[x_i, y_i, z_i \mid i = 1, 2, \ldots]$. Let ν be the derivation of K given by the rule

$$x_i^{\nu} = x_{i+1}, \; y_i^{\nu} = y_{i+1}, \; z_i^{\nu} = z_{i+1} \quad \text{for all} \quad i = 1, 2, \ldots .$$

Clearly for all $x \in R$ there exists a homomorphism of Φ-algebras $\phi_x = \phi : K \to R$ such that $\phi(z_i) = \phi(z_1^{\nu^i}) = r^{\delta^i}$, $\phi(y_i) = 0$ and $\phi(x_i) = \phi(x_1^{\nu^i}) = x^{\delta^i}$. Since $\phi(P_{p,i,\nu}(z_1)) = P_{p,i,\delta}(r)$, it is enough to prove that $P_{p,i,\nu}(z_1) = 0$. We set $z = z_1$. Then according to 5.15 we have

$$r^{(\nu z)^p} = r^{\nu^p} z^p + \sum_{i=2}^{p-1} r^{\nu^i} P_{p,i,\nu}(z) + r^{\nu} T_{p,\nu}(z),$$

for all $r \in K$. In particular,

$$\begin{aligned} (x_1 y_1)^{(\nu z)^p} &= (x_1 y_1)^{\nu^p} z^p + \sum_{i=2}^{p-1} (x_1 y_1)^{\nu^i} P_{p,i,\nu}(z) \\ &\quad + (x_1 y_1)^{\nu} T_{p,\nu}(z), \end{aligned} \tag{5.16}$$

$$\begin{aligned} x_1^{(\nu z)^p} &= x_1^{\nu^p} z^p + \sum_{i=2}^{p-1} x_1^{\nu^i} P_{p,i,\nu}(z) \\ &\quad + x_1^{\nu} T_{p,\nu}(z), \qquad (5.17) \\ y_1^{(\nu z)^p} &= y_1^{\nu^p} z^p + \sum_{i=2}^{p-1} y_1^{\nu^i} P_{p,i,\nu}(z) \\ &\quad + y_1^{\nu} T_{p,\nu}(z), \qquad (5.18) \end{aligned}$$

Multiplying (5.17) by y_1 and (5.18) by x_1 we obtain

$$\begin{aligned} x_1^{(\nu z)^p} y_1 &= x_1^{\nu^p} y_1 z^p + \sum_{i=2}^{p-1} x_1^{\nu^i} y_1 P_{p,i,\nu}(z) \\ &\quad + x_1^{\nu} y_1 T_{p,\nu}(z), \qquad (5.19) \\ x_1 y_1^{(\nu z)^p} &= x_1 y_1^{\nu^p} z^p + \sum_{i=2}^{p-1} x_1 y_1^{\nu^i} P_{p,i,\nu}(z) \\ &\quad + x_1 y_1^{\nu} T_{p,\nu}(z). \qquad (5.20) \end{aligned}$$

Since ν^p and $(\nu z)^p$ are derivations, substracting (5.19) and (5.20) from (5.16), we obtain

$$\sum_{i=2}^{p-1} \left[(x_1 y_1)^{\nu^i} - x_1^{\nu^i} y_1 - x_1 y_1^{\nu^i} \right] P_{p,i,\nu}(z) = 0.$$

From the Leibnitz formula and the definition of the derivation ν we infer that

$$\begin{aligned} 0 &= \sum_{i=2}^{p-1} \left[\sum_{j=1}^{i-1} \binom{i}{j} x_1^{\nu^j} y_1^{\nu^{i-j}} \right] P_{p,i,\nu}(z) \\ &= \sum_{i=2}^{p-1} \left[\sum_{j=1}^{i-1} \binom{i}{j} x_{j+1} y_{i-j+1} \right] P_{p,i,\nu}(z). \end{aligned}$$

The coefficient of $x_2 y_i$ in this polynomial is equal to $\binom{i}{1} P_{p,i,\nu}(z)$. Since $\binom{i}{1} = i \neq 0$, $P_{p,i,\nu}(z) = 0$.

Therefore

$$x_1^{(\nu z)^p} = x_1^{\nu^p} z^p + x_1^{\nu} T_{p,\nu}(z). \tag{5.21}$$

Let $x \in R$. Applying ϕ_x we infer from (5.21) that $x^{(\delta r)^p} = x^{\delta^p} r^p + x^{\delta} T_{p,\delta}(r)$ for all $x \in R$. In particular $x^{(\mu c)^p} = x^{\mu^p} c^p + x^{\mu} T_{p,a}(c)$ for all $x \in H$ and so $(\mu c)^p = \mu^p c^p + \mu T_{p,a}(c)$. Since $\mu = ad(a)|_H$, **(a)** is proved.

(b) We let K be the polynomial ring with derivation ν as defined in **(a)** and consider the skew polynomial ring $K[t;\nu]$, where $kt = tk + k^{\nu}$ for all $k \in K$. Obviously $\nu = ad(t)|_K$. Since K is commutative, it follows from Lemma 5.2.1 and (5.21) that

$$\begin{aligned} ad((tz)^p)|_K &= (ad(tz)|_K)^p = (ad(t)|_K z)^p \\ &= (ad(t)|_K)^p z^p + ad(t)|_K T_{p,\nu}(z). \end{aligned}$$

Hence $[x_1, (tz)^p] = [x_1, t^p] z^p + [x_1, t] T_{p,\nu}(z)$ and

$$[x_1, (tz)^p - t^p z^p - t T_{p,\nu}(z)] = 0.$$

We claim that $(tz)^p - t^p z^p - t T_{p,\nu}(z) = 0$. Assume the contrary. Clearly $(tz)^p - t^p z^p - t T_{p,\nu}(z) = \sum_{i=1}^n t^i k_i$, where $k_i \in \Phi[z_i;\ i = 1, 2, \ldots]$, $n < p$ and $k_n \neq 0$. Note that $n > 0$ and the coefficient of t^{n-1} in $[x_1, (tz)^p - t^p z^p - t T_{p,\nu}(z)]$ is equal to $n x_2 k_n + x_1 k_{n-1} \neq 0$ which contradicts $[x_1, (tz)^p - t^p z^p - t T_{p,\nu}(z)] = 0$. Therefore $(tz)^p - t^p z^p - t T_{p,\nu}(z) = 0$. Define the mapping $\psi : K[t;\nu] \to A$, setting $\psi(t) = a$ and $\psi(k) = \phi_x(k)$ for all $k \in K$. The reader may now easily verify that ψ is a homomorphism of Φ-algebras. Thus $(ac)^p - a^p c^p - a T_{p,a}(c) = \psi\left((tz)^p - t^p z^p - t T_{p,\nu}(z)\right) = 0$.

(c) By Lemma 5.2.1 we have $(a + c)^p = a^p + c^p + W(a, c)$, where $W(x, y)$ is a sum of Lie monomials of degree p in x, y. Since F is commutative, all Lie monomials in which c appears twice are equal to zero. So $W(a, c) = m \cdot ad(a)^{p-1}(c)$ for some integer m. Therefore we have

$$\begin{aligned} [a, (a + c)^p] &= [a, a^p] + [a, c^p] + m \left[a, ad(a)^{p-1}(c)\right] \\ &= -m \cdot ad(a)^p(c). \end{aligned}$$

On the other hand,

$$\begin{aligned} [a,(a+c)^p] &= [\ldots[[a,a+c],a+c],\ldots,a+c] \\ &= [\ldots[[a,c],a+c],\ldots,a+c] \\ &= [\ldots[[a,c],a],\ldots,a] \\ &= -ad(a)^p(c). \end{aligned}$$

Therefore $m \cdot ad(a)^p(c) = ad(a)^p(c)$ and we are done.

Definition 5.4.3 *A triple $(K;F;\Lambda)$ is said to be a restricted differential F-Lie algebra (p-DL-algebra), if the following condition holds:*

(a) *$(K;F;\Lambda)$ is a differential F-Lie algebra;*

(b) *K is a restricted Lie algebra over Φ with a p-operation $\delta \mapsto \delta^{[p]}$ satisfying the following identity:*

$$(\delta c)^{[p]} = \delta^{[p]}c^p + \delta T_{p,\delta}(c),$$

where $T_{1,\delta}(c) = c$, $T_{n+1,\delta}(c) = c(T_{n,\delta})^{\hat{\delta}}$, and $c \in F/Ann_F(K)$, $\delta \in K$.

(c) *the mapping Λ is a homomorphism of restricted Lie Φ-algebras.*

For a p-SDL-algebra $L \subset A$ and the mapping $\Lambda : A \to Der(1 \cdot F)$ given by the rule $c^{\Lambda(a)} = [c,a]$ for all $a \in A$ and $c \in 1 \cdot F$, we infer from Corollary 5.2.2 and Lemma 5.4.2 that $(L;F;\Lambda)$ is a p-DL-algebra.

In what follows $\hat{\mu} = \Lambda(\mu)$ for a p-DL-algebra K and $\mu \in K$.

Definition 5.4.4 *Let K and L be p-DL-algebras over Φ. Then a mapping $f : K \to L$ is said to be a homomorphism of p-DL-algebras if it is a homomorphism of DL-algebras and a homomorphism of restricted Lie algebras (i.e. $\left(\delta^{[p]}\right)^f = \left(\delta^f\right)^{[p]}$ for all $\delta \in K$).*

Notions of cover algebras, enveloping algebras and the universal enveloping algebras for p-DL-algebras are defined analogously to corresponding notions for restricted Lie algebras and DL-algebras.

Now we are in a position to describe a universal enveloping algebra $(U(K); \rho)$ of a p-DL-algebra K as a factor of a free Φ-algebra in the case when F is a free Φ-module and K is a free right F-module. Let X be a basis of the right F-module K and G a basis of F over Φ. We set $Z = \{\bar{g} \mid g \in G\} \cup \{\bar{x}\bar{g} \mid x \in X,\ g \in G\}$. Let $S = S{<}Z{>}$ be the free semigroup (with 1), $\Phi{<}Z{>}$ the free Φ-algebra (with 1) generated by the set Z and L the Φ-span of Z in $\Phi{<}Z{>}$. Denote by K' the differential F-Lie algebra $K \oplus F$ (see Lemma 5.3.5) and let $\psi : K' \to L$ be the Φ-map given by the rule $g \mapsto \bar{g}$, $xg \mapsto \bar{x}\bar{g}$ for all $g \in G$ and $x \in X$. Obviously ψ is an isomorphism of Φ-modules. We define $I(K)$ to be the ideal of $\Phi{<}Z{>}$ generated by $\bar{e} - 1$ and all elements of the form

$$(ua)^\psi - u^\psi a^\psi,\ [u,v]^\psi - \left[u^\psi, v^\psi\right],\ \left(k^{[p]}\right)^\psi - \left(k^\psi\right)^p$$

for all $a \in G$, $u, v \in K'$ and $k \in K$. Further letting I be the ideal of $\Phi{<}Z{>}$ generated by $\bar{e} - 1$ and all elements of the form

$$(ba)^\psi - \bar{b}\bar{a},\ (xa)^\psi - \bar{x}\bar{a},\ [x,y]^\psi - [\bar{x},\bar{y}],$$
$$[x,a]^\psi - \left(a^{\hat{x}}\right)^\psi,\ \left(k^{[p]}\right)^\psi - \left(k^\psi\right)^p$$

we claim that $I = I(K)$. Indeed, letting ν denote the projection of $\Phi{<}Z{>}$ onto $U = U(K) = \Phi{<}Z{>}/I$, we set $\rho = \psi\nu$ and $M = L^\nu = K'^\rho$. It was shown before the proof of Theorem 5.3.6 that F^ρ is a subalgebra of U containing the identity 1 and ρ induces a homomorphism $F \to F^\rho$. Moreover U and M have a canonical F-module structure via ρ, M is a special differential F-Lie algebra and ρ is a homomorphism of DL-algebras. Before the proof of Theorem 5.2.3 it was shown that $\left(u^{[p]}\right)^\rho = (u^\rho)^p$ for all $u \in K$. Now it is clear that $I = I(K)$.

Consider any cover $((A;N);f)$ of the p-DL-algebra K. Define the mapping $f' : K' \to N+1\cdot F$, setting $(k+c)^{f'} = k^f+1\cdot c$ for all $k \in K$, $c \in F$. It follows easily from the definitions that $((A;N);f')$ is a cover of the DL-algebra K'. Lift f' to a homomorphism $\sigma : \Phi{<}Z{>}\to A$. Recall that f' is a homomorphism of right F-modules and Lie algebras over Φ. Furthermore, $\left(k^{[p]}\right)^{f'} = \left(k^{f'}\right)^{[p]}$ for all $k \in K$. Hence $I(K)^{f'} = 0$ and f' induces a homomorphism $\phi : U \to A$ such that $\rho\phi = f'$. Thus U is a universal enveloping algebra of the p-DL-algebra K.

Now we are ready to prove the main theorem of this section.

Theorem 5.4.5 *Let $(K;F;\Lambda)$ be a p-DL-algebra with the universal enveloping algebra $(U(K);\phi)$, assuming that F is a free Φ-module and K is a free right F-module with a well-ordered basis X. Then the set*

$$\begin{aligned} V = \{x_1^\phi x_2^\phi \dots x_m^\phi \mid x_j \in X,\ x_1 \le x_2 \le \dots \le x_m \quad \textit{and} \\ \textit{if} \quad x_k = x_{k+1} = \dots = x_{k+s-1}, \quad \textit{then} \quad s < p\} \cup \{1\} \end{aligned}$$

is a basis of the right F-module $U(K)$ (we shall refer to V as a PBW-basis of the universal enveloping algebra $U(K)$ of the p-DL-algebra K).

Proof. Without loss of generality we may assume that G is well-ordered. Define a well-ordering on the set $Z = \{\bar{x} \mid x \in X\} \cup \{\bar{g} \mid g \in G\}$, setting $\bar{u} < \bar{v}$ if either $u, v \in X$ and $u < v$, or $u, v \in G$ and $u < v$, or $u \in X$ and $v \in G$, for all $\bar{u}, \bar{v} \in Z$.

We continue with the same notations as in Theorems 5.1.1, 5.2.3 and 5.3.6. Consider the reduction system Δ of $\Phi{<}Z{>}$,

$$\begin{aligned} \sigma_{yx} &= \left(\bar{y}\bar{x}, \bar{x}\bar{y} + [y,x]^\psi\right), \quad \text{for all} \quad y > x \in X; \\ \chi_{gx} &= \left(\bar{g}\bar{x}, \bar{x}\bar{g} + \left(g^{\hat{x}}\right)^\psi\right), \quad \text{for all} \quad g \in G,\ x \in X; \\ \omega_{gq} &= \left(\bar{g}\bar{q}, (gq)^\psi\right), \quad \text{for all} \quad g, q \in G; \end{aligned}$$

$$\begin{aligned}\pi_e &= (\bar{e}, 1)\,;\\ \sigma_x &= \left(\bar{x}^p, x^{[p]\psi}\right) \quad \text{for all} \quad x \in X.\end{aligned}$$

Letting $\leq$ denote the linear order on S which was introduced in the proof of Theorem 5.1.1 we note that this ordering is a semigroup one compatible with the reduction system Δ and satisfying the descending chain condition. Further, let $I = I(\Delta)$ be the ideal of the algebra $\Phi{<}Z{>}$ generated by the reduction system Δ.

We claim that all ambiguities of Δ are resolvable and the set

$$\begin{aligned}V' = \{&\bar{x}_1\bar{x}_2\ldots\bar{x}_m\bar{g} \mid x_j \in X,\ g \in G,\ x_1 \leq x_2 \leq \ldots \leq x_m\\ &\text{and if } x_k = x_{k+1} = \ldots = x_{k+s-1}, \text{ then } s < p\} \cup \bar{G}\end{aligned}$$

is a Φ-basis of $\Phi{<}Z{>}_{irr}$.

Indeed, consider the various ambiguities. It was shown in the proof of Theorem 5.1.1 that the following ambiguity is resolvable.

Case 1. Overlap ambiguity $(\sigma_{zy}, \sigma_{yx}, \bar{z}, \bar{y}, \bar{x})$, where $x, y, z \in X$ and $z > y > x$.

It was shown in the proof of Theorem 5.3.6 that the ambiguities listed below in cases 2-7 are resolvable.

Case 2. Overlap ambiguity $(\chi_{gy}, \sigma_{yx}, \bar{g}, \bar{y}, \bar{x})$, where $x, y \in X$, $g \in G$ and $y > x$.

Case 3. Overlap ambiguity $(\omega_{hg}, \sigma_{gx}, \bar{h}, \bar{g}, \bar{x})$, where $x \in X$, $g, h \in G$.

Case 4. Inclusion ambiguity $(\pi_e, \chi_{ex}, \bar{e}, \bar{x})$, where $x \in X$.

Case 5. Overlap ambiguity $(\omega_{gp}, \omega_{pq}, \bar{g}, \bar{p}, \bar{q})$, where $g, p, q \in G$.

Case 6. Inclusion ambiguity $(\pi_e, \omega_{eg}, \bar{e}, \bar{g})$, where $g \in G$.

Case 7. Inclusion ambiguity $(\omega_{ge}, \pi_e, \bar{g}, \bar{e})$, where $g \in G$.

In the proof of Theorem 5.2.3 we showed that the ambiguities listed below in cases 8-10 are resolvable.

Case 8. Overlap ambiguity $(\sigma_{yx}, \sigma_x, \bar{y}, \bar{x}, \bar{x}^{p-1})$, where $x, y \in X$ and $y > x$.

Case 9. Overlap ambiguity $(\sigma_x, \sigma_{xy}, \bar{x}^{p-1}, \bar{x}, \bar{y})$, where $x, y \in X$ and $x > y$.

Case 10. Overlap ambiguity $(\sigma_x, \sigma_x, \bar{x}^l, \bar{x}^{p-l}, \bar{x}^l)$, where $x \in X$.

Case 11. Overlap ambiguity $(\chi_{gx}, \sigma_x, \bar{g}, \bar{x}, \bar{x}^{p-1})$, where $g \in G$ and $x \in X$. We set $v = R_{\chi_{gx}x^{p-1}}(\bar{g}\bar{x}^p) = \bar{x}\bar{g}\bar{x}^{p-1} + g^{\hat{x}\psi}\bar{x}^{p-1}$ and $w = R_{g\sigma_x}(\bar{g}\bar{x}^p) = \bar{g}x^{[p]\psi}$. By Lemma 5.3.8 there exists a sequence R of reductions such that $R(v) = \bar{x}^p\bar{g} + Ad(\bar{x})^p(\bar{g})$. Obviously $R_{\sigma_x g}R(v) = x^{[p]\psi}\bar{g} + Ad(\bar{x})^p(\bar{g})$. It follows from (5.10) that $R'(w) = x^{[p]\psi}\bar{g} + g^{\widehat{x^{[p]}}\psi}$ for some sequence of reductions R'. Since K is a p-DL-algebra, $ad(x)^p(g) = g^{\widehat{x^{[p]}}}$. Thus $R_{\sigma_x g}R(v) = R'(w)$ and this ambiguity is resolvable.

The Diamond Lemma may therefore be invoked, and in view of Lemma 1.3.2 we again conclude that V' is a Φ-basis for $U(K)$. It follows that V is a right F-module basis of $U(K)$.

Corollary 5.4.6 *Let $(K; F; \Lambda)$ be a p-DL-algebra with the universal enveloping algebra $(U(K); \phi)$. Assume that F is a free Φ-module, and K is a free right F-module. Then $\rho : K \to U(K)^{(-)}$ is a monomorphism of differential restricted Lie algebras.*

As in Section 5.3 we make the following

Definition 5.4.7 *Let K, L be restricted differential Lie algebras and let $\tau : F/Ann_F(K) \to F/Ann_F L$ be an isomorphism of Φ-algebras. Then a mapping $f : K \to L$ is said to be a τ-semilinear homomorphism of p-DL-algebras, if the following conditions hold:*

(a) f is a homomorphism of restricted Lie Φ-algebras;

(b) $(\delta c)^f = \delta^f c^\tau$ for all $\delta \in K$, $c \in F/Ann_F(K)$;

(c) $\widehat{\delta^f} = \tau^{-1}\hat{\delta}\tau$ for all $\delta \in K$.

The following statements are proved analogously to Proposition 5.3.10 and Corollary 5.3.11

Proposition 5.4.8 *Let $(K; F; \Lambda)$ be a p-DL-algebra, $(U(K); \rho)$ the universal enveloping algebra of K, $L \subseteq A$ a special restricted differential F-Lie algebra over Φ and $h : K \to L$ a τ-semilinear homomorphism of p-DL-algebras. Then there is a unique homomorphism $h' : U(K) \to A$ of Φ-algebras such that $\rho h' = h$ and $h'(uc) = h'(u)(c + Ann_F(K))^\tau$ for all $u \in U(K)$, $c \in F$.*

As in Section 5.3 we note that in case F is a field the ideal $Ann_F(K) = 0$ where it appears in Definition 5.4.7 and Proposition 5.4.8.

Corollary 5.4.9 *Let $(K; F; \Lambda)$ be a p-DL-algebra with the universal enveloping algebra $(U(K); \phi)$. Then for any τ-semilinear automorphism $h : K \to K$ of DL-algebras there exists a unique τ-semilinear automorphism $h' : U(K) \to U(K)$ of algebras such that $\rho h' = h\rho$.*

5.5 A Particular Differential Lie Algebra

The preceding sections of this chapter were devoted to proving a generalized PBW theorem for abstract differential Lie algebras. In this book, however, we will be mainly interested in a particular differential Lie algebra, one which arises from the set $Der(R)$ of derivations of prime ring R.

Let R be a prime ring with extended centroid C, prime field Φ, and symmetric ring of quotients Q. We let $Der(R)$ denote the Φ-Lie algebra of derivations of R. We have previously seen (Proposition 2.5.1) that any derivation of R can be uniquely extended in an obvious way to a derivation of Q, and so we may regard $Der(R) \subseteq Der(Q) \subseteq End_\Phi(Q)$. We mention here that it is useful to view C as left multiplications acting on Q. For $c \in C$ and $\delta \in Der(R)$ δc is clearly a derivation of Q and so

$Der(Q)$ is a right C-space. For $q \in Q$ we see from

$$0 = [c, q]^\delta = [c^\delta, q] + [c, q^\delta] = [c^\delta, q]$$

that δ induces a derivation on C which we denote by $\hat{\delta}$. From

$$q^{c\delta} = (cq)^\delta = c^\delta q + cq^\delta = q^{c^\delta} + q^{\delta c}$$

we have the important commutation formula in $End(Q)$:

$$c\delta = \delta c + c^{\hat{\delta}}, \quad \delta \in Der(Q),\ c \in C. \tag{5.22}$$

The set $D_i = \{ad(a) \mid a \in Q\}$ of all inner derivations of Q is a C-Lie algebra and also a Lie ideal of $Der(Q)$ (in fact, $[ad(a), \delta] = ad(a^\delta)$, $\delta \in Der(Q)$). The subset of $Der(Q)$ we are primarily interested in is

$$D = D(R) = (Der(R))C + D_i \tag{5.23}$$

From the preceding observations it is clear that $D(R)$ is a special differential C-Lie algebra over Φ with cover $End(Q)$.

Suppose $char(C) = p$. From Remark 1.1.1(b) we see that $Der(R)$ is closed under pth powers and from Lemma 5.2.1(a) that D_i is closed under pth powers as well. For $\delta \in Der(R)$ and $c \in C$ we see from Lemma 5.4.2(b) that $(\delta c)^p \in (Der(R))C$ and consequently from Lemma 5.2.1(c) that $D(R)$ is a special restricted differential C-Lie algebra over Φ with cover $End(Q)$.

Now let U be the (restricted) universal enveloping algebra of D and pick an ordered right C-basis $\mathcal{B}$ of D. Then by Theorem 5.3.6 and Theorem 5.4.5 U has a (restricted) PBW right C-basis induced by $\mathcal{B}$. By Corollary 5.3.7 and Corollary 5.4.6 the canonical mapping of D into U is injective and so (with some abuse of notation) we may identify D with its image in U. On the other hand $D \subseteq End_\Phi(Q)$ whence there is a C-ring map $\rho : U \to End(Q)$ such that the following diagram is commutative:

$$\begin{tikzcd}
D \arrow[rr] \arrow[dr] & & U \arrow[dl, "\rho"] \\
& End(Q) &
\end{tikzcd}$$

Thus there is a copy of D in both U and $End(Q)$, each designated by D, and the context will always make it clear which copy of D we are using.

If σ is an automorphism of C and K, L are any differential C-Lie algebras we recall from Definition 5.3.9 and Definition 5.4.7 the notion of a σ-semilinear differential Lie map $f : K \to L$ (the key features are $(\delta c)^f = \delta^f c^\sigma$ and $\widehat{\delta^f} = \sigma^{-1}\hat{\delta}\sigma$). Then $f : K \to L^*$ is an ordinary differential Lie map, where L^* is simply L made into a new differential C-Lie algebra by defining $\delta \cdot c = \delta c^\sigma$ and $\tilde{\delta} = \sigma^{-1}\hat{\delta}\sigma$. These considerations, of course, apply in particular to the case $K = D$. For instance, any σ-semilinear differential C-Lie map of D into itself can, in view of Proposition 5.3.10 and Proposition 5.4.8, be uniquely extended to a σ-semilinear Φ-algebra homomorphism of U into itself.

In the sequel it will be important to choose the basis $\mathcal{B}$ of D so that it reflects the nature of D. To this end let $\mathcal{B}_0$ be a well-ordered right C-basis for D modulo D_i and $\mathcal{B}_i$ a well-ordered C-basis for D_i. Then, taking $\mathcal{B}_0 < \mathcal{B}_i$, we see that $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_i$ is a well-ordered right C-basis for D. Let $\mathcal{W}$ be the PBW right C-basis of U relative to $(\mathcal{B}, <)$ as provided by Theorem 5.3.6 and Theorem 5.4.5. If $\Delta = \delta_{i_1}\delta_{i_2}\ldots\delta_{i_n}$, $\delta_{i_j} \in \mathcal{B}$, then the length $|\Delta|$ of Δ is m, the number of factors. $\mathcal{W}$ is then ordered as follows: if $|\Delta| < |\Gamma|$ then $\Delta < \Gamma$ and if $|\Delta| = |\Gamma|$ then the ordering is lexicographic. We remark that the well-ordering of $\mathcal{B}$ implies that $\mathcal{W}$ is also well-ordered. We denote by $\mathcal{W}_0$ the set of all elements of $\mathcal{W}$ whose factors lie in $\mathcal{B}_0$ (and also including 1) and by $\mathcal{W}_i$ the subset of $\mathcal{W}$ arising from $\mathcal{B}_i$. It is an easy exercise to show that $U_i = U(D_i)$ may be taken to be the subring of $U(D)$ generated by C and D_i and $\mathcal{W}_i$ is the PBW basis of U_i with respect to $(\mathcal{B}_i, <)$.

Finally, from the definition of U, we note that the commutation formula corresponding to (5.22) is also valid in U:

$$c\delta = \delta c + c^{\hat{\delta}}, \quad \delta \in D \subseteq U,\ c \in C \subseteq U. \tag{5.24}$$

Setting $\Delta = \delta_1\delta_2 \ldots \delta_n$, $\delta_i \in D \subseteq U$ and referring the reader to the notations preceding Remark 1.1.1 we have the following useful formula in U for slipping an element $c \in C$ through Δ:

$$c\Delta = \sum_{s} \Delta_s c^{\widehat{\Delta_{s'}}} \tag{5.25}$$

The proof is a formal inductive one making repeated use of (5.24) and we omit it. However, to give the reader a concrete illustration of the formula (5.25) when written out in detail, we write out the case $n = 3$ in full:

$$\begin{aligned} c\delta_1\delta_2\delta_3 &= \delta_1\delta_2\delta_3 c + \delta_1\delta_2 c^{\hat{\delta}_3} + \delta_1\delta_3 c^{\hat{\delta}_2} + \delta_2\delta_3 c^{\hat{\delta}_1} \\ &+ \delta_1 c^{\hat{\delta}_2\hat{\delta}_3} + \delta_2 c^{\hat{\delta}_1\hat{\delta}_3} + \delta_3 c^{\hat{\delta}_1\hat{\delta}_2} + c^{\hat{\delta}_1\hat{\delta}_2\hat{\delta}_3}. \end{aligned}$$

Of course, using the map $\rho : U \to End(Q)$, the formula in $End(Q)$ corresponding to (5.25) is also valid.

This Page Intentionally Left Blank

Chapter 6

Rings with Generalized Polynomial Identities

6.1 Prime GPI-rings

It is hoped that much of the material developed in the first five chapters is of interest in its own right. However, it must also be said that the choice of these topics was to a large extent dictated by the background requirements of the remaining chapters, in which the structure theory for generalized identities is laid out and some applications are given.

Although there were earlier scattered examples of situations where "generalized identities" appeared (e.g., [248], [194]), for all intents and purposes the subject began in 1965 with the appearance of Amitsur's fundamental paper [3] characterizing primitive rings satisfying a so-called generalized polynomial identity (this notion, abbreviated as GPI, will presently be formally defined). In 1969 Martindale simultaneously generalized Amitsur's theorem on primitive GPI-rings and Posner's theorem on prime PI-rings [205], obtaining a characterization of prime GPI-rings. Our main purpose in the present section is to present a proof (due to C.-L. Chuang) of this result.

Let R be a prime ring with extended centroid C and symmetric ring of quotients Q. We let X be an (infinite) set and form the coproduct $Q_C{<}X{>}$ of the C-algebra Q and the free algebra $C{<}X{>}$ over C. If P is any C-algebra with 1 containing Q then, in view of Remark 1.2.5, any set-theoretic map $X \to P$ can be extended uniquely to a C-algebra map $Q_C{<}X{>}\to P$ such that $q \mapsto q$, $q \in Q$. Such a map will be called a *substitution*. Given an element $\phi = \phi(x_1, x_2, \ldots, x_n) \in Q_C{<}X{>}$ and elements $p_1, p_2, \ldots, p_n \in P$, $\phi(p_1, p_2, \ldots, p_n)$ will denote the image of ϕ under the substitution determined by $x_i \mapsto p_i$. Let $0 \neq U$ be an additive subgroup of R. An element $\phi = \phi(x_1, x_2, \ldots, x_n) \in Q_C{<}X{>}$ is said to be a *generalized polynomial identity on U* if $\phi(u_1, u_2, \ldots, u_n) = 0$ for all $u_1, u_2, \ldots, u_n \in U$. Henceforth we will use the abbreviation GPI, and (with some grammatical license) make statements such as "ϕ is a GPI on U" or "U is GPI".

We first look at linear elements of $Q_C < X >$ in a single variable x, i.e., elements of QxQ, and make the following

Remark 6.1.1 *$Q_{(l)}Q_{(r)} \cong Q \otimes_C Q \cong QxQ$ as C-spaces, with the isomorphisms given by $\alpha : l_a r_b \mapsto a \otimes b$, $\beta : a \otimes b \mapsto axb$, $a, b \in Q$.*

Proof. We know already by Theorem 2.3.6 that α is an isomorphism and clearly β is a well defined surjection. If $\phi = \sum_i a_i \otimes b_i \in \ker(\beta)$, then $\sum_i a_i x b_i = 0$ whence $\sum_i a_i q b_i = 0$ for all $q \in Q$, i.e., $\sum_i l_{a_i} r_{b_i} = 0$, and so $\sum_i a_i \otimes b_i = 0$ in view of the isomorphism α.

Lemma 6.1.2 *Let $0 \neq \phi = \sum_{i=1}^m a_i x b_i \in QxQ$. Then:*

(i) For all nonzero ideals I of R $\phi(I) \neq 0$;

(ii) If $0 \neq I \lhd R$ is such that $\dim_C(\phi(I)C) < \infty$ then there exist nonzero elements $a, b \in R$ such that $\dim_C(aRCb) < \infty$.

Proof. Without loss of generality we may assume that $m \geq 1$ and that $\{a_i\}$ and $\{b_i\}$ are each C-independent sets. By Theorem 2.3.3 there exists $\beta = \sum_k l_{u_k} r_{v_k} \in R_{(l)}R_{(r)}$ such that $a_1 \cdot \beta \neq 0$ but $a_i \cdot \beta = 0$, $i > 1$. We set $\psi(x) = \sum_k u_k \phi(v_k x)$ and note that $\psi(x) = a' x b_1$ where $a' = a_1 \cdot \beta \neq 0$. Let $0 \neq I \triangleleft R$ and suppose $\phi(I) = 0$. Then $\psi(I) = 0$ whence we have the contradiction $a' I b_1 = 0$. Part **(i)** has thereby been proved. Now suppose $0 \neq I \triangleleft R$ is such that $\dim_C(\phi(I)C) < \infty$. Since $u_k\phi(v_k I) \subseteq u_k \phi(I)$, it follows that $dim_C(\psi(I)C) < \infty$ that is, $\dim_C(a' I b_1 C) < \infty$. Pick $s \in I$ such that $0 \neq a = a's \in R$ and $t \in R$ such that $0 \neq b = tb_1 \in R$. As a result we see that $aRb \subseteq a'Ib_1$ and accordingly $\dim_C(aRbC) < \infty$. The proof of **(ii)** is thereby complete.

Lemma 6.1.2 yields the immediate

Corollary 6.1.3 *If $\phi \in QxQ$ is a GPI on some $0 \neq I \triangleleft R$ then $\phi = 0$, i.e., there are no nonzero linear GPI's in one variable.*

The next lemma continues where the preceding lemma left off.

Lemma 6.1.4 *Let $A = RC$ be the central closure of R and let $a, b \in A$ be nonzero elements such that $\dim_C(aAb) < \infty$. Then the ring A has a nonzero idempotent e such that eA is a minimal right ideal of A and $\dim_C(eAe) < \infty$ (In particular A is a primitive ring with nonzero socle).*

Proof. Without loss of generality we may assume that the elements $a, b \in A$ are such that $\dim_C(aAb) \leq \dim_C(uAv)$ for all nonzero $u, v \in A$. We claim that $M = aAbA$ is a minimal right ideal of A. Indeed, since A is prime and $a \neq 0 \neq b$, $M \neq 0$. Let $0 \neq z = \sum_i a x_i b y_i \in M$ where $x_i, y_i \in A$. Setting $u = \sum_i x_i b y_i$, we note that $z = au$. Further we have $auAb \subseteq aAb$ and so $auAb = aAb$ by the choice of a, b. Hence $auAbA = M$ and hence

$$M = auAbA \subseteq zA \subseteq M \quad \text{and} \quad zA = M$$

for all nonzero $z \in M$. Therefore M is a minimal right ideal of A. By Proposition 4.3.3 $M = eA$ for some idempotent e and eAe is a division ring. Clearly $e = \sum_{i=1}^{m} au_i bv_i$. Hence $eAe \subseteq \sum_{i=1}^{m} aAbv_i$ and so $\dim_C(eAe) < \infty$, and the lemma is proved.

Before taking up the matter of arbitrary GPI's we shall first describe the linearization process in $Q_C{<}X{>}$. We mention that this process works equally well for $Q = Q_{mr}$ as for $Q = Q_s$. We fix a C-basis $\mathcal{A}$ of Q containing 1 which in conjunction with the usual C-basis of $C{<}X{>}$ leads to the monomial basis $\mathcal{M}(\mathcal{A})$ of $Q_C{<}X{>}$. For $M \in \mathcal{M}(\mathcal{A})$ we define

$$\begin{aligned}
\deg_x(M) &= \text{number of times } x \text{ appears in } \quad M; \\
\deg(M) &= \sum_{x \in X} \deg_x(M); \\
ht_x(M) &= \max\{\deg_x(M) - 1, 0\}; \\
ht(M) &= \sum_{x \in X} ht_x(M) \\
&= \deg(M) \text{ minus the number of distinct } x\text{'s} \\
&\quad\ \text{appearing in } M.
\end{aligned}$$

Now we write

$$\phi = \phi(x_1, x_2, \ldots, x_n) = \sum_M c_M M \in Q_C{<}X{>},$$
$$M \in \mathcal{M}(\mathcal{A}),\ c_M \in C.$$

We shall say that M *belongs* to ϕ if $c_M \neq 0$. We define:

$$\begin{aligned}
\deg_x(\phi) &= \max\{\deg_x(M) \mid c_M \neq 0\}; \\
\deg(\phi) &= \max\{\deg(M) \mid c_M \neq 0\}; \\
ht_x(\phi) &= \max\{ht_x(M) \mid c_M \neq 0\}; \\
ht(\phi) &= \max\{ht(M) \mid c_M \neq 0\}.
\end{aligned}$$

Given $k > 0$ and $x \in X$ we say that ϕ is *k-homogeneous in x* if $\deg_x(M) = k$ for each M belonging to ϕ. Given a sequence

$\tau = (m_1, m_2, \ldots, m_n)$ of nonegative integers we say that ϕ is *τ-homogeneous* if ϕ is m_i-homogeneous in x_i, $i = 1, 2, \ldots, n$. If, in addition, each $m_i = 1$ we say that ϕ is *multilinear of degree n.* Clearly, given $x \in X$ appearing in ϕ, we may write ϕ uniquely as a sum $\sum_{k=0}^{m} \phi_k(x)$, ϕ_k k-homogeneous in x, $m = \deg_x(\phi)$. Also we may write ϕ uniquely as a sum $\sum \phi_\tau$ where ϕ_τ is τ-homogeneous.

Let $\phi \neq 0$ be of degree n and suppose $\deg_x(\phi) = m > 1$ for some $x \in X$. We can then perform the following operation which we shall refer to as an operation of type A. Notationally suppressing all $x_i \neq x$ appearing in ϕ we shall write $\phi = \phi(x)$. Let M belong to ϕ such that $\deg_x(M) = m$ and write

$$M = M(x) = P_{i_0} x P_{i_1} \ldots x P_{i_m}$$

where $P_{i_j} \in \mathcal{M}(\mathcal{A})$ does not contain x. Choose $y \in X$ not appearing in ϕ and form

$$\psi = \phi(x + y) - \phi(x) - \phi(y).$$

One observes in particular that the monomial

$$P_{i_0} x P_{i_1} \ldots x P_{i_{m-1}} y P_{i_m}$$

belongs to ψ, thereby showing

$$(i)\ \deg(\psi) = \deg(\phi) \quad \text{(and hence } \psi \neq 0)$$

Furthermore it is clear that

(ii) $\deg_x(\psi) = m - 1 = \deg_y(\psi)$;
(iii) $\deg_{x_i}(\psi) \leq \deg_{x_i}(\phi)$, $x_i \neq x, y$;
(iv) $ht(\psi) < ht(\phi)$ (because of **(ii)**);
(v) If ϕ is a *GPI* then ψ is a *GPI.*

An operation of type B may be performed in case there is an $x \in X$ appearing in ϕ but not in each M belonging to ϕ.

Here we simply replace ϕ by the element ρ obtained from ϕ by sending x to 0. Clearly $\rho \neq 0$, $\deg(\rho) \leq \deg(\phi)$, $ht(\rho) \leq ht(\phi)$, and if ϕ is a GPI, then ρ is a GPI.

We say that ψ is a *linearization of* ϕ if ψ is multilinear and is obtained from ϕ by a finite sequence of operations of types A and B. Evidently every $\phi \neq 0$ has a linearization and as a result we have

Remark 6.1.5 *If $0 \neq \phi$ is a GPI on I of degree n then there exists a nonzero multilinear GPI on I of degree $\leq n$.*

We are now in a position to prove the main result of this section (which we shall sometimes in the future refer to as "the prime GPI theorem"). The proof we give is due to Chuang [87] who greatly simplified the original proof in [205].

Theorem 6.1.6 *Let R be a prime ring with extended centroid C and central closure $A = RC$. Then there is a nonzero GPI ϕ on I for some $0 \neq I \lhd R$ if and only if A has a nonzero idempotent e such that eA is a minimal right ideal of A (hence A is primitive with nonzero socle) and eAe is a finite dimensional division algebra over C.*

Proof. If $\dim_C(eAe) = n < \infty$ and St_{n+1} is the standard polynomial in $n+1$ variables, then

$$\phi = St_{n+1}(ex_1e, ex_2e, \ldots, ex_{n+1}e)$$

is the required a GPI.

Conversely let $0 \neq \phi$ be a GPI on some $0 \neq I \lhd R$. By Remark 6.1.5 we may assume that $\phi = \phi(x_1, x_2, \ldots, x_n)$ is multilinear of degree n. Pick any C-basis $\mathcal{A}$ of Q. The element ϕ, when written in terms of the monomial basis $\mathcal{M}(\mathcal{A})$, only involves a *finite* subset F of $\mathcal{A}$. By suitable reordering of the variables we may write

$$\phi = b_0x_1 \ldots b_{n-2}x_{n-1}\psi(x_n) + \sum \alpha_M M + \sum \beta_N N + \sum \gamma_P P,$$

$\alpha_M, \beta_N, \gamma_P \in C$ where

(*i*) $0 \neq \psi(x_n) \in Qx_nQ$;

(*ii*) M is of the form $b'_0x_1 \dots b'_{n-2}x_{n-1}\chi(x_n)$, with $(b'_0, \dots, b'_{n-2}) \neq (b_0, \dots, b_{n-2})$ and $\chi(x_n) \in Qx_nQ$;

(*iii*) N is of the form $b''_0x_1 \dots b''_{i-1}x_ib''_ix_nb''_{i+1}x_{i+1} \dots b''_{n-1}x_{n-1}b''_n$;

(*iv*) $x_1, x_2, \dots, x_{n-1}$ appear in a different order in P.

By Lemma 6.1.4 we may assume that $\psi(I)C \not\subseteq V = \sum_{d \in F} dC$. Choose $r \in I$ such that $\psi(r) \notin V$ and set

$$\rho(x_1, x_2, \dots, x_{n-1}) = \phi(x_1, x_2, \dots, x_{n-1}, r).$$

Let $\mathcal{A}'$ be a C-basis of Q containing $F \cup \{\psi(r)\}$, and consider ρ as being written in terms of the monomial basis $\mathcal{M}(\mathcal{A}')$ of $Q_C\!<\!X\!>$ induced by $\mathcal{A}'$. It is then clear that the monomial $H = b_0x_1 \dots b_{n-2}x_{n-1}\psi(r)$ cannot be canceled by any monomials which arise from M, N, or P. For instance, N ends in $b''_n \in F$ whereas H ends in $\psi(r) \notin F$. Thus $0 \neq \rho$ is a GPI of degree $n-1$ on I, and so by induction the proof is complete.

Although in this section our framework is that of the symmetric ring of quotients Q_s, the following corollary shows that the effect of a GPI carries up to the maximal right ring of quotients Q_{mr}.

Corollary 6.1.7 *Let R be a prime ring with extended centroid C, central closure $A = RC$ and $Q = Q_{mr}(R)$. Then the following conditions are equivalent:*

(i) *There is a nonzero GPI ϕ on I for some $0 \neq I \lhd R$;*

(ii) *Any subring $A \subseteq H \subseteq Q$ is primitive with nonzero socle and a nonzero idempotent $e \in H$ such that eHe is a finite dimensional division algebra over C;*

(iii) The ring Q is isomorphic to the complete ring of linear transformations of a right vector space over a division ring which is finite dimensional over its center;

(iv) R is GPI.

Proof. **(i)** $\Rightarrow$ **(ii)** By Theorem 6.1.6 A has nonzero socle and **(ii)** then follows immediately from Theorem 4.3.6(**ii**).

(ii) $\Rightarrow$ **(iii)** By Lemma 2.1.9, $Q = Q_{mr}(H)$. Now the statement **(iii)** follows from the symmetric version of Theorem 4.3.7 (**viii**).

(iii) $\Rightarrow$ **(iv)** We identify the ring Q with this complete ring of linear transformations over a division ring Δ. Let n be the dimension of Δ over its center and let e be an idempotent of rank 1 of the linear transformation ring Q. Clearly $eQe \cong \Delta$. Hence the generalized polynomial

$$\phi = St_{n+1}(ex_1e, \ldots, ex_{n+1}e) = St_{n+1}(ex_1, \ldots, ex_{n+1})e$$

where St_{n+1} is the standard polynomial in $(n+1)$ variables vanishes under all substitutions $x_i \mapsto q_i \in Q$, $i = 1, 2, \ldots, n+1$. Pick any $a \in (e : R)_R$ such that $ea \neq 0$. Then

$$0 \neq \psi = St_{n+1}(eax_1, eax_2, \ldots, eax_{n+1})ea \in Q_C{<}X{>}$$

is a *GPI* on R. The implication **(iv)** $\Rightarrow$ **(i)** is obvious. The proof is thereby complete.

Theorem 6.1.6 says that prime *GPI* rings are "well-behaved", but for non *GPI* prime rings we have the following positive result which will prove useful in the sequel.

Lemma 6.1.8 *Let R be a prime ring, let U be an additive subgroup of R which is not GPI, and fix $x \in X$. Let $T_i = \{\phi_{ij}(x) \mid j = 1, 2, \ldots, n_i\}$, $i = 1, 2, \ldots, m$, be m given subsets of $Q_C{<}X{>}$ each of which is C-independent. Then there exists $u \in U$ such that the subset $T_i(u) = \{\phi_{ij}(u) \mid j = 1, 2, \ldots, n_i\} \subseteq Q$ is C-independent for each $i = 1, 2, \ldots, m$.*

Proof. Suppose to the contrary that for each $u \in U$ there exists $1 \leq i \leq m$ such that $T_i(u)$ is a C-dependent subset of Q. Then the set

$$T_i(u, v_i) = \{\phi_{ij}(u)v_i \mid j = 1, 2, \ldots, n_i\}$$

remains a C-dependent subset of Q for all $v_i \in U$. We form the element

$$\phi = \prod_{i=1}^{m} St_{n_i}(\phi_{i1}(x)y_i, \phi_{i2}(x)y_i, \ldots, \phi_{in_i}(x)y_i)z_i$$

where $y_1, \ldots, y_m, z_1, \ldots, z_m \in X$ (distinct from x) and St_{n_i} is the standard polynomial in n_i variables. Clearly $\phi \neq 0$ but, since $St_k(a_1, a_2, \ldots, a_k) = 0$ whenever $a_1, a_2, \ldots, a_k$ are C-dependent, ϕ is a GPI on U, contrary to our hypothesis.

We close this section by showing how Theorem 6.1.6, with assistance from other results we have obtained, implies the pathbreaking theorems of Kaplansky [137], Amitsur [3], and Posner [242].

Let us take a closer look at the situation when R is a primitive GPI ring. By Theorem 6.1.6, RC has a nonzero socle $Soc(RC)$ and so by Theorem 4.3.6(**ii**) R has socle $Soc(R) = Soc(RC)$. Furthermore Theorem 6.1.6 assures us of a minimal idempotent e (necessarily in R) such that $eRe = eRCe$ is finite dimensional over C, and we know from Theorem 4.3.7(**ix**) that eRe has center isomorphic to C.

The fundamental theorem of Amitsur ([3], Theorem 10), which in essence originated the theory of generalized polynomial identities in 1965, follows immediately from the preceding paragraph.

Theorem 6.1.9 (Amitsur) *Let R be a primitive ring with extended centroid C. Then R is GPI if and only if R contains a minimal idempotent e such that* $\dim_C(eRe) < \infty$.

Now we recall that a ring R is called a PI-ring if there exists a nonzero element $f(x_1, x_2, \dots, x_n) \in C{<}X{>}$ which vanishes under all substitutions $x_i \mapsto r_i \in R$, $1 \le i \le n$. Next suppose that R is a primitive PI ring over C with faithful irreducible right R-module M and $D = End(M_R)$. We may assume without loss of generality that R has a multilinear polynomial identity

$$f(x_1, x_2, \dots, x_n) = \sum_{\sigma \in S_n} \lambda_\sigma x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(n)}$$

of degree n with $\lambda_1 = 1$. Then

$$x_1 x_2 \dots x_n \in \sum_{\sigma \in S_n \setminus \{1\}} \lambda_\sigma x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(n)} R$$

is a pivotal monomial of R. By Theorem 4.4.3 we have that $R = End_D(M)$ where $\dim_D(M) < \infty$. On the other hand our preceding remarks show that $\dim_C(D) < \infty$. We have thereby completed the proof of Kaplansky's Theorem [137], which originated the theory of polynomial identities in 1948.

Theorem 6.1.10 (Kaplansky) *Let R be a primitive ring with extended centroid C. Then R is PI over C if and only if R is finite dimensional central simple over C.*

Finally, we come to Posner's Theorem [242] of 1960, which became a fundamental tool in the theory of prime rings (an area which had recently been opened up by Goldie's Theorems). We state and prove the original version. Here we recall that given a ring R, a ring $S \supseteq R$ with 1 is said to be a *two-sided classical ring of quotients* of R if all regular element (i.e., nonzero divisors) of R are invertible in S and for every $s \in S$ there exist regular elements $t_1, t_2 \in R$ such that $st_1, t_2 s \in R$.

Theorem 6.1.11 (Posner) *Let R be a prime ring with extended centroid C. Then R is PI over C if and only if $A = RC$ is a two-sided classical ring of quotients of R and* $\dim_C(A) < \infty$.

Proof. We may assume that the *PI* is multilinear and hence satisfied by A. By Theorem 6.1.6, A is a primitive ring with nonzero socle and so by Kaplansky's Theorem $A = M_n(D)$ for some $n \geq 1$, where D is a division algebra finite dimensional over its center C. Let $e_1, e_2, \ldots, e_n$ be the usual diagonal matrix units. We now claim that every nonzero ideal U of R contains a regular element of A. We may choose a nonzero ideal W of R such that $W \subseteq U$, $We_i \subseteq U$ and $e_iW \subseteq U$ for all i, whence $0 \neq e_iW^3e_i \subseteq U$. Selecting $0 \neq u_i \in e_iW^3e_i \subseteq U$, we see that $u = u_1 + u_2 + \ldots + u_n \in U$ has rank n and so must be a regular element of A. Now let $a \in A$, choose a nonzero ideal U of R such that $aU + Ua \subseteq R$, and by the preceding claim select a regular element $b \in U$. Clearly $ab, ba \in R$. Next let $d \in R$ be a regular element. Suppose $dx = 0$ for some $x \in A$. Choose a nonzero ideal V of R such that $xV \subseteq R$. Then $d(xV) = 0$ and so $xV = 0$. Hence $x = 0$ and $r_A(d) = 0$. Analogously one may show that $l_A(d) = 0$. Therefore d is a regular element of A. Since $\dim_C(A) < \infty$, every regular element of A is invertible. It follows that every regular element of R is invertible in A and thus A is a two-sided classical ring of quotients of R.

It must be added that our methods do not enable us to prove the sharper version of Posner's Theorem, namely, the one that asserts additionally that C is the field of fractions of the center of R. This latter improvement stems from the existence of central polynomials in $M_n(F)$ (see Formanek [105] and Razmyslov [246]) and was proved by Rowen [255].

As a final note we mention that in section 6.3, where our main purpose will be to study *GPI*'s in semiprime rings, we shall at the same time also broaden the definition of a *GPI* to allow its coefficients to lie in Q_{mr} (rather than just in Q_s). As we shall see the theory will not be weakened by this generalization since the fundamental prime *GPI* theorem will remain intact.

6.2 Identities with a Fixed Antiautomorphism

The first step in extending the notion of *GPI*'s for prime rings to that of more general identities in prime rings was taken in [207], [208] and [257] where R was a prime ring with involution $*$ satisfying an identity of the form $\phi(x_1, \ldots, x_n, x_1^*, \ldots, x_n^*)$. The special case of an ordinary *GPI* satisfied by the symmetric elements was studied by Martindale [208] and the more general situation by Rowen [257] (also independently by Skinner [265]).

Our motivation for including this topic in the present chapter (rather than delegating it to Chapter 7 as a special case of a far more general situation) is severalfold. First, some readers may be primarily interested in rings with involution but not in further generality. Secondly, this particular theory has important applications in its own right (e.g., in Chapter 9 the solution of Herstein's Lie isomorphism problem uses it in a crucial way). Thirdly, the lemma on linear identities (Lemma 6.2.1) forms an important step in reducing the general theory in Chapter 7 to the prime *GPI* theorem (Theorem 6.1.6). Lastly, it is hoped that the exposition in this section will help in a small way to bridge the gap between section 6.1 and the vastly more complicated setting in Chapter 7.

For the remainder of this section R will denote a prime ring with a fixed antiautomorphism g. This includes the special case when g is an involution. The arguments required for the general antiautomorphism case are essentially no different from those needed in the involution case. We have previously noted (section 2.5) that g may be uniquely extended to an antiautomorphism of the symmetric ring of quotients $Q = Q_s(R)$. Let X be an arbitrary infinite set, let $X^g = \{x^g \mid x \in X\}$ be a copy of X with the elements suggestively superscripted by g, and let $X \cup X^g$ be the disjoint union of these two sets. We then form the coproduct

$Q_C{<}X \cup X^g{>}$ of Q and the free algebra $C{<}X \cup X^g{>}$ over C.

As in the preceding section any set-theoretic map of $X \cup X^g$ into a C-algebra P containing Q can be uniquely lifted to a C-algebra map of $Q_C{<}X \cup X^g{>} \to P$ such that $q \mapsto q$, $q \in Q$. Such maps are called substitutions. We will be primarily interested in the situation where $P = Q$ or $P = Q_C{<}X \cup X^g{>}$. As the notation for the set X^g suggests, it is natural to focus on substitutions of $Q_C{<}X \cup X^g{>}$ into Q which are restricted by the requirement $x^g \mapsto r^g$ whenever $x \mapsto r$, $r \in Q$. Such substitutions will be called *g-substitutions* . Let U be an additive subgroup of R. Then an element $\phi = \phi(x_1, \dots, x_n, x_1^g, \dots, x_n^g) \in Q_C{<}X \cup X^g{>}$ is said to be a *g-identity on* U if ϕ is mapped to 0 under all g-substitutions for which $x_i \mapsto r_i$, $r_i \in U$ (Our main concern is the situation in which $0 \neq U = I \lhd R$).

We begin with a seemingly very specialized result, but as it turns out one which plays a key role in the proof of Theorem 7.5.8 (as well as Theorem 6.2.3). We fix $x \in X$ and set $L_x = QxQ + Qx^gQ$.

Lemma 6.2.1 *Let g be an antiautomorphism of R and let*

$$0 \neq \phi(x) = \sum_{i=1}^{m} a_i x b_i + \sum_{j=1}^{n} c_j x^g d_j \in L_x$$

be such that $\dim_C(\phi(I)C) < \infty$ *for some* $0 \neq I \lhd R$. *Then R is GPI (in particular if ϕ is a g-identity on I then R is GPI).*

Proof. The proof is by induction on n. The case $n = 0$ is obvious in view of Lemma 6.1.2, Lemma 6.1.4 and Theorem 6.1.6. We assume that the lemma is true for $n-1$ and show it for n. Without loss of generality we may assume that $m > 0$ and the elements $a_1, a_2, \dots, a_m$ are C-independent. Therefore $c_n x a_1, \dots, c_n x a_m, a_1, \dots, a_m$ are C-independent elements of $Q_C{<}X \cup X^g{>}$. By Corollary 6.1.7 it is enough to consider the case when I is not GPI. By Lemma 6.1.8 there exists $r \in I$ such that

$$c_n r a_1, \dots, c_n r a_m, a_1, \dots, a_m \quad \text{are } C\text{-independent.} \qquad (6.1)$$

Then we have

$$\begin{aligned}
\phi'(x) &= \phi(x c_n^{g^{-1}} r^{g^{-1}}) - c_n r \phi(x) \\
&= \sum_{i=1}^{m} a_i x c_n^{g^{-1}} r^{g^{-1}} b_i + \sum_{j=1}^{n} c_j r c_n x^g d_j \\
&\quad - \sum_{i=1}^{m} c_n r a_i x_i b_i - \sum_{j=1}^{n} c_n r c_j x^g d_j \\
&= \sum_{i=1}^{m} a_i x c_n^{g^{-1}} r^{g^{-1}} b_i - \sum_{i=1}^{m} c_n r a_i x_i b_i \\
&\quad + \sum_{j=1}^{n-1} (c_j r c_n - c_n r c_j) x^g d_j.
\end{aligned}$$

From (6.1) it follows that $\phi'(x) \neq 0$. Clearly $\phi'(I)C \subseteq \phi(I)C + c_n r \phi(I)C$ and so $dim_C(\phi'(I)C) < \infty$. Therefore by induction the proof is complete.

Before taking up the matter of arbitrary g-identities we describe a linearization process compatible with g. With only a few adjustments it is similar to the usual linearization process described in the previous section and we will omit most of the details. For a nonzero monomial M in $Q_C{<}X \cup X^g{>}$ we define the g-degree of M in x (g-$\deg_x(M)$) to be the number of times x or x^g appears in M. Similarly we define the *g-height of M in x* (g-$ht_x(M)$) to be $\max\{g\text{-}\deg_x(M) - 1, 0\}$ and the g-height of M (g-$ht(M)$) to be $\sum_{x \in X} g\text{-}ht_x(M)$. For example if

$$M = a_0 x_2 a_1 x_2^g a_2 x_3^g a_3 x_2^g a_4$$

then g-$\deg_{x_2}(M) = 3$, g-$\deg_{x_3}(M) = 1$ and

$$\deg_{x_2}(M) = 1, \ \deg_{x_2^g}(M) = 2, \ \deg_{x_3}(M) = 0, \ \deg(M) = 4.$$

We say that ϕ is *g-multilinear* of degree n in $x_1, x_2, \ldots, x_n$ if for each monomial M in ϕ and each i we have $g\text{-deg}_{x_i}(M) = 1$ and $\deg(M) = n$. For example $x_1 a x_2^g + x_2^g b x_1^g$ is g-multilinear of degree 2 in x_1 and x_2 but is not multilinear. On the other hand $x_1 a x_1^g$ is multilinear of degree 2 in x_1, x_1^g but is not g-multilinear. With these adjustments in mind, together with the fact that g is additive, a process similar to that described in the preceding section results in

Remark 6.2.2 *If $0 \neq \phi$ is a g-identity of degree n on $0 \neq I \lhd R$ then there exists a nonzero g-multilinear identity on I of degree $\leq n$.*

Theorem 6.2.3 *Let R be a prime ring with an antiautomorphism g, and let $0 \neq \phi \in Q_C{<}X \cup X^g{>}$ be a g-identity on I, where $0 \neq I \lhd R$. Then R is GPI.*

Proof. In view of Remark 6.2.2 we may assume that $\phi = \phi(x_1, \ldots, x_n, x_1^g, \ldots, x_n^g)$ is g-multilinear of degree n in $x_1, \ldots, x_n$. Let $r_2, r_3, \ldots, r_n \in I$ and set

$$\psi(x_1) = \phi(x_1, r_2, r_3, \ldots, r_n, x_1^g, r_2^g, r_3^g, \ldots, r_n^g).$$

We note that $\psi \in L_{x_1}$ is a g-identity on I. If $\psi \neq 0$, then by Lemma 6.2.1 R is GPI. Therefore we may assume without loss of generality that for every choice of $r_2, r_3, \ldots, r_n \in I$

$$\phi(x_1, r_2, r_3, \ldots, r_n, x_1^g, r_2^g, r_3^g, \ldots, r_n^g)$$

is the zero element of $Q_C{<}X{>}$. In particular

$$\phi(r_1, r_2, r_3, \ldots, r_n, s_1, r_2^g, r_3^g, \ldots, r_n^g) = 0$$

for all $r_1, \ldots, r_n, s_1 \in I$. Continuing this process with $x_2, \ldots, x_n$ we may eventually assume that

$$\phi(r_1, r_2, r_3, \ldots, r_n, s_1, s_2, \ldots, s_n) = 0$$

for all $r_i, s_i \in I$, $i = 1, 2, \ldots, n$, i.e., $\phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$ is a GPI on I.

As an important special case we have the

Corollary 6.2.4 *If R is a prime ring with involution $*$ and $0 \neq \phi$ is a $*$-identity on $0 \neq I \lhd R$ then R is GPI.*

Included in this corollary are the following special cases.

Corollary 6.2.5 *Let R be a prime ring of characteristic different from 2 with involution $*$ with skew elements K and symmetric elements S.*

(i) If K is GPI, then R is GPI.

(ii) If S is GPI, then R is GPI.

Proof. In either **(i)**, or **(ii)** let $0 \neq \phi(x_1, x_2, \ldots, x_n)$ be a GPI. Then

$$\psi = (x_1 - x_1^*, x_2 - x_2^*, \ldots, x_n - x_n^*)$$

is a $*$-identity on R in case **(i)** and

$$\psi = (x_1 + x_1^*, x_2 + x_2^*, \ldots, x_n + x_n^*)$$

is $*$-identity on R in case **(ii)**. By Corollary 6.2.4 R is GPI.

6.3 Semiprime GPI-rings

Our main purpose in the present section is the extension of the notion of generalized polynomial identities to semiprime rings. At the same time, as promised at the end of section 6.1, we will extend the definition of GPI so that the coefficients may lie in Q_{mr}. It is debatable which ring of quotients is better to use. On the one hand Q_s is a less complicated ring not as far removed from R as is Q_{mr}, and working with (dense) two-sided ideals is generally a simpler matter than working with dense right ideals. In Chapter 7 we shall choose to use Q_s. On the other hand, Q_{mr} has the advantage of more generality and also has the useful property that if J is a dense right ideal of R then for any subring $J \subseteq S \subseteq Q_{mr}(R)$ we have $Q_{mr}(S) = Q_{mr}(R)$. Also Q_{mr} includes classical rings of quotients not included in Q_s, e.g., for R a simple right Ore domain $Q_s = R$ whereas Q_{mr} coincides with the classical ring of right quotients. At any rate for the remainder of this chapter we elect to use Q_{mr} instead of Q_s, and we proceed to define the notion of GPI in this wider sense.

Let R be a semiprime ring with extended centroid C and maximal right ring of quotients $Q = Q_{mr}(R)$. Letting X be an infinite set, we form the coproduct $Q_C{<}X{>}$ of the free C-algebra $C{<}X{>}$ and Q. As we already know any set-theoretic map $X \to Q$ can be extended uniquely to a C-algebra map $Q_C{<}X{>} \to Q$ such that $q \mapsto q$ for all $q \in Q$. As usual we will call such a map a substitution. Now let $0 \neq U$ be an additive subgroup of R. An element $\phi = \phi(x_1, x_2, \ldots, x_n) \in Q_C{<}X{>}$ (where $Q = Q_{mr}(R)$) is said to be a *generalized polynomial identity* on U if $\phi(u_1, u_2, \ldots, u_n) = 0$ for all $u_1, u_2, \ldots, u_n \in U$.

Before beginning our investigation of GPI's in the general semiprime setting we shall first establish the reassuring fact that in the prime case no weakening of the theory has taken place.

Remark 6.3.1 *Let R be a prime ring with extended centroid C and $Q = Q_{mr}(R)$. Further let $q_1, q_2, \ldots, q_n \in Q$ be C-independent and $J = \cap_{i=1}^{n}(q_i : R)_R$. Then either* $\dim_C(RC) < \infty$, *or there exists an element $r \in J$ such that $q_1r, q_2r, \ldots, q_nr$ are C-independent elements.*

Proof. Suppose that $q_1r, q_2r, \ldots, q_nr$ are C-dependent for all $r \in J$. Consider the C-linear mappings $l_{q_i} : V = JC \to RC$ given by the left multiplications by q_i. By Amitsur's Lemma there exist elements $c_1, c_2, \ldots, c_n$ such that $\tau = \sum_{i=1}^{n} c_i l_{q_i}$ is a nonzero linear transformation of finite rank (see Theorem 4.2.7). Setting $q = \sum_{i=1}^{n} c_i q_i$, we note that $\tau = l_q$. Hence $K = qJC$ is a nonzero finite dimensional right ideal of RC. Since RC is a prime ring, $RC \subseteq End_C(qJC)$ which proves our remark.

Corollary 6.3.2 *Let R be a prime ring with extended centroid C, $Q = Q_{mr}(R)$, $Q_s = Q_s(R)$ and $0 \neq \phi \in Q_C{<}X{>}$ a GPI on a nonzero ideal U of R. Then U has a nonzero generalized polynomial identity $\psi \in Q_{sC}{<}X{>}$.*

Proof. Pick any C-basis $\mathcal{A}$ of Q containing 1 and consider the monomial basis $\mathcal{M}(\mathcal{A})$ of $Q_C{<}X{>}$. The element ϕ, when written in terms of the monomial basis $\mathcal{M}(\mathcal{A})$, involves only a finite subset $b_1, \dots, b_m$ of $\mathcal{A}$. If $\dim_C(RC) = k < \infty$, then R is a PI-ring and then $St_{k+1}(x_1, x_2, \dots, x_{k+1}) \in \psi \in Q_{sC}{<}X{>}$ is a GPI of R. Suppose $\dim_C(RC) = \infty$. By Remark 6.3.1 there exists an element $r \in R$ such that $b_1 r, b_2 r, \dots, b_m r$ are C-independent elements of $A = RC$. Write $\phi = \sum_{i=1}^{k} \alpha_i M_i$ where $M_i \in \mathcal{M}(\mathcal{A})$ and $\alpha_i \in C$. It follows that

$$M_i(rx_1, \dots, rx_n)r \neq M_j(rx_1, \dots, rx_n)r \quad \text{for} \quad i \neq j.$$

Therefore $\phi(rx_1, rx_2, \dots, rx_n)r$ is a nonzero GPI on U with coefficients belonging to A, and the proof is complete.

The preceding corollary, in conjunction with Theorem 6.1.6, yields

Corollary 6.3.3 *Let R be a prime ring with extended centroid C, $Q = Q_{mr}(R)$ and $\phi = \phi(x_1, x_2, \dots, x_n) \in Q_C{<}X{>}$ a nonzero GPI on R. Then the central closure $A = RC \subseteq Q$ contains a nonzero idempotent e such that eAe is a finite dimensional division C-algebra (Hence A is a primitive ring with nonzero socle).*

Corollary 6.3.3 tells us that if a prime ring is GPI in the "wider" sense then it is GPI in the sense of section 6.1. We will, however, in the course of the present section establish the analogues of Corollary 6.1.3 (Lemma 6.3.12), Theorem 6.2.3 (Theorem 6.3.18), and Lemma 6.1.8 (Corollary 6.3.14) for prime rings.

We return now to the investigation of GPI's in semiprime rings and make the following important definition. A GPI $\phi \in Q_C{<}X{>}$ is called *strict*, if $r_C(\phi) = 0$. The following example shows us the importance of the condition $r_C(\phi) = 0$.

Example. Let K be any commutative semiprime ring with an identity e and let A be any semiprime ring. We set $R = K \oplus A$ and $u = (e, 0)$. Then $\phi(x, y) = uxy - uyx$ is a GPI of R and $r_C(\phi) = (1 - u)C$. Thus the GPI ϕ only contains nontrivial information about a "part" of R, namely about the direct summand K of R. We shall see that in general the situation is analogous to that of the example.

Remark 6.3.4 *$Q_C{<}X{>}$ is a nonsingular C-module. In particular for any $\phi \in Q_C{<}X{>}$ there exists a unique idempotent $E(\phi) \in C$ such that $r_C(\phi) = (1 - E(\phi))C$.*

Proof. Let A be the set of all finite sequences of elements of X. For any $\alpha = (x_1, x_2, \ldots, x_m), \beta = (y_1, y_2, \ldots, y_n) \in A$ we set $|\alpha| = m + 1$ and $\alpha \cup \beta = (x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n) \in A$. Given any natural number n, we define $Q^{[n]}$ to be the n-fold tensor product $Q \otimes_C Q \otimes_C \ldots \otimes_C Q$ of Q. Now we set

$$Q_\alpha = Q^{[|\alpha|]} \quad \text{and} \quad H = \oplus_{\alpha \in A} Q_\alpha .$$

We note that for $\tau = \emptyset$, $|\tau| = 1$ and $Q_\tau = Q$. Define a multiplication in H by the rule

$$\begin{aligned}&(q_1 \otimes \ldots \otimes q_m \otimes q_{m+1})(p_1 \otimes p_2 \otimes \ldots \otimes p_{n+1})\\ &= q_1 \otimes \ldots \otimes q_m \otimes (q_{m+1} p_1) \otimes p_2 \otimes p_{n+1} \in Q_{\alpha \cup \beta},\end{aligned}$$

and its consequences, where

$$\alpha = (x_1, x_2, \dots, x_m), \beta = (y_1, y_2, \dots, y_n) \in A,$$
$$q_1 \otimes \dots \otimes q_m \otimes q_{m+1} \in Q_\alpha \quad \text{and}$$
$$p_1 \otimes p_2 \otimes \dots \otimes p_{n+1} \in Q_\beta.$$

Now we define a mapping $f : Q_C{<}X{>} \rightarrow H$ by the rule

$$q_1x_1q_2 \dots x_mq_{m+1} \mapsto q_1 \otimes q_2 \otimes \dots \otimes q_{m+1} \in Q_\alpha$$

and its consequences, where $\alpha = (x_1, \dots, x_m)$. We leave it to the reader to check the straightforward details that H is an associative C-algebra and f is an isomorphism of C-algebras. Since a direct sum of nonsingular C-modules is a nonsingular C-module and Q is a nonsingular C-module by Corollary 3.1.2, it is enough to show that the tensor product of nonsingular C-modules is nonsingular as well. To this end consider nonsingular C-modules M and N. Let $z = \sum_{i=1}^m x_i \otimes y_i \in M \otimes N$ where $x_i \in M$, $y_i \in N$. We set $M' = \sum_{i=1}^m Cx_i$ and $N' = \sum_{i=1}^m Cy_i$. According to Remark 3.1.4 and Lemma 3.1.1, the C-modules M' and N' are isomorphic to direct sums of principal ideals of the ring C and are injective C-modules. In particular they are direct summands of M and N respectively. The reader can easily check that the operation of tensor product commutes with the operation of direct sum. Hence $M' \otimes_C N'$ is a direct summand of $M \otimes_C N$ and furthermore the C-module $M' \otimes_C N'$ is isomorphic to a direct sum of tensor products of principal ideals of C. Therefore it is enough to show that $U = (Cu) \otimes_C (Cv)$ is a nonsingular C-module for all idempotents $u, v \in C$. Consider the mapping $h : Cu \times Cv \rightarrow Cuv$ given by the rule $(xu, yv) \mapsto xyuv$, $x, y \in C$. Clearly h is a balanced mapping. Hence there exists a homomorphism of C-modules $F : U \rightarrow Cuv$ such that $F(xu \otimes yv) = xyuv$ for all $x, y \in C$. Obviously F is a surjective homomorphism. Further let $z = \sum x_iu \otimes y_iv \in U$ where $x_i, y_i \in C$. Then $z = (\sum x_iy_iuv) \otimes v$ and so F is injective. Thus

$U \cong Cuv$ is a nonsingular C-module and our remark now follows from Lemma 3.1.1.

Let $\phi \in Q_C{<}X{>}$ be a GPI on R, $e = E(\phi)$, $I = (e : R)_R$ and $J = eI$. Since e is a central element of Q, I is a dense ideal of R. Setting $K = (1-e)I$, we note that K is an ideal of R, $K \cap J = 0$ and $I = J \oplus K$. Using Proposition 2.1.10 one checks that

$$Q = Q_{mr}(J \oplus K) = Q_{mr}(J) \oplus Q_{mr}(K) = eQ \oplus (1-e)Q,$$

$Q_{mr}(J) = eQ$ and $eQ_C{<}X{>}= (eQ)_{eC}{<}X{>}$. Hence

$$\phi \in eQ_C{<}X{>}= (eQ)_{eC}{<}X{>}$$

is a strict GPI on the ring J and determines a zero generalized polynomial identity on the ring K.

These comments show that in the study of semiprime rings with GPI's one may confine one's attention to strict GPI's.

There are two ways to characterize semiprime rings with strict GPI's. The first one is using the results of section 2.3 and the skeleton of the proof of Theorem 6.1.6 to give a direct proof of a semiprime ring version of the prime GPI theorem. This approach was used in [21] and [22]. The second possibility is using the method of orthogonal completion to derive the desired description from the prime GPI theorem. We will follow this approach in order to demonstrate the method of orthogonal completion.

Let R be a semiprime ring with extended centroid C, $Q = Q_{mr}(R)$, $Q_s = Q_s(R)$, and $A = RC \subseteq Q_s$. We let $D = O(R)$, $H = O(A)$ denote the orthogonal completions of R and A, noting (by Proposition 3.1.10) that $O(Q) = Q$ and $O(Q_s) = Q_s$. Further let $B = B(C)$, $P \in Spec(B)$, and let $\phi_P : Q \to Q/PQ = \overline{Q}$ be the canonical surjection of rings. By Theorem 3.2.7 $\overline{D} = \phi_P(D)$ is a prime ring, and by Theorem 3.2.15**(iv)** $\overline{C} = \phi_P(C)$ is the extended centroid of $\overline{D}$. By Theorem 3.2.15**(i)** $\overline{Q} \subseteq Q_{mr}(\overline{D})$

and by Theorem 3.2.15(**iii**) $\overline{D}\,\overline{C} \subseteq \overline{H} \subseteq \overline{Q_s} \subseteq Q_s(\overline{D})$. The following remark shows that the canonical C-algebra map

$$\Phi_P : Q_C\text{<}X\text{>} \to \overline{Q}_{\overline{C}}\text{<}X\text{>} \subseteq Q_{mr}(\overline{D})_{\overline{C}}\text{<}X\text{>}$$

behaves properly.

Remark 6.3.5 *Let R be a semiprime ring with extended centroid C, $B = B(C)$ the Boolean ring of all idempotents of C, $Q = Q_{mr}(R)$, $F = Q_C\text{<}X\text{>}$ and P a maximal ideal of B. Further let $\phi_P : Q \to Q/PQ = \overline{Q}$ be the canonical homomorphism of C-algebras and $\Phi_P : F \to \overline{Q}_{\overline{C}}\text{<}X\text{>}$ the canonical extension of ϕ_P. Then:*

(i) Φ_P is a surjective homomorphism with $\ker(\Phi_P) = PF$;

(ii) If $\psi \in Q_C < X >$, then $\psi \in$ $\ker(\Phi_P)$ *if and only if $E(\psi) \in P$.*

Proof. (**i**) Let M and N be nonsingular left C-modules. We set $\overline{M} = M/PM$ and $\overline{N} = N/PN$. Consider the mapping $g : M \times N \to \overline{M} \otimes_{\overline{C}} \overline{N}$ given by the rule

$$(m, n) \mapsto (m + PM) \otimes (n + PN),\ m \in M,\ n \in N.$$

Clearly g is balanced. Therefore there exists a mapping

$$G : M \otimes_C N \to \overline{M} \otimes_{\overline{C}} \overline{N}$$

such that

$$m \otimes n \mapsto (m + PM) \otimes (n + PN),\ m \in M,\ n \in N.$$

We claim that $\ker(G) = P(M \otimes_C N)$. Indeed,

$$P(M \otimes_C N) = (PM) \otimes_C N = M \otimes_C (PN).$$

Note that $\overline{M}$ and $\overline{N}$ are vector spaces over the field $\overline{C}$. Pick subsets $\{u_\gamma \mid \gamma \in \Gamma\} \subseteq M$ and $\{v_\delta \mid \delta \in \Delta\} \subseteq N$ such that

$\{u_\gamma + PM \mid \gamma \in \Gamma\}$ and $\{v_\delta + PN \mid \delta \in \Delta\}$ are $\overline{C}$-bases of $\overline{M}$ and $\overline{N}$ respectively. Let $z = \sum_i x_i \otimes y_i \in M \otimes_C N$ where $x_i \in M$, $y_i \in N$. Obviously $z = \sum_{\gamma,\delta} c_{\gamma\delta} u_\gamma \otimes v_\delta + z'$ where $c_{\gamma\delta} \in C$ and $z' \in P(M \otimes_C N)$. If $z \notin P(M \otimes_C N)$, then $c_{\gamma_0\delta_0} \notin P$ for some $\gamma_0 \in \Gamma$, $\delta_0 \in \Delta$. Since $\{(u_\gamma + PM) \otimes (v_\delta + PN) \mid \gamma \in \Gamma, \delta \in \Delta\}$ is a $\overline{C}$-basis of $\overline{M} \otimes_{\overline{C}} \overline{N}$, we conclude that $G(z) \neq 0$. Therefore $\ker(G) = P(M \otimes_C N)$.

Taking into account the isomorphism of the C-algebras H and $Q_C{<}X{>}$ established in the proof of the preceding remark, we infer now that $\ker(\Phi_P) = PF$.

(ii) The proof is similar to that of Remark 3.2.2.

Returning to our general setting we suppose now that

$$\psi = \psi(x_1, x_2, \ldots, x_n) \in Q_C{<}X{>}$$

is a strict GPI on R. We claim that $\overline{\psi} = \Phi_P(\psi)$ is a nonzero GPI on $\overline{D}$. Indeed, it follows from Remark 3.1.8 and Remark 3.1.9 that ψ is a strict GPI on D. For any $d_1, d_2, \ldots, d_n \in D$ we have

$$\overline{\psi}(\phi_P(d_1), \ldots, \phi_P(d_n)) = \phi_P(\psi(d_1, \ldots, d_n)) = 0$$

and so $\overline{\psi}$ is a GPI on $\overline{D}$. Since $E(\psi) = 1$, $\Phi_P(\psi) \neq 0$ by Remark 6.3.5. We summarize what we have proved in the following

Corollary 6.3.6 *Let R be a semiprime ring with extended centroid C, $B = B(C)$, $Q = Q_{mr}(R)$, $D = O(R)$ the orthogonal completion of R and P a maximal ideal of B. Further let $\phi_P : Q \to Q/PQ = \overline{Q}$ and $\Phi_P : Q_C{<}X{>} \to \overline{Q}_{\overline{C}}{<}X{>}$ be canonical homomorphisms of C-algebras and let $\psi \in Q_C{<}X{>}$ be a strict GPI on R. Then $\Phi_P(\psi)$ is a nonzero GPI on the prime ring $\phi_P(D)$.*

An idempotent e of a C-algebra A is said to be of *finite C-rank n* if eAe is a free C-module with a basis of n elements.

Further, an idempotent e is called *abelian* if eAe is a von Neumann regular ring all of whose idempotents are central. Finally an idempotent $e \in A$ is called *faithful* (or *C-faithful* for emphasis) if $r_C(e) = 0$. The notion of a faithful abelian idempotent e of finite C-rank n lends itself very nicely to the following description by Horn formulas:

$$\begin{aligned}
\chi_0(e,c) &= \|c \in C\| \wedge (\|c = 0\| \vee \|ce \neq 0\|) \wedge \|e^2 = e\|;\\
\chi_1(e,x_1,x_2) &= \|(ex_1e)(ex_2e)(ex_1e) = ex_1e\|;\\
\chi_2(e,y_1,y_2) &= \|(ey_1e)^2 \neq ey_1e\|\\
&\quad \vee\|(ey_1e)(ey_2e) = (ey_2e)(ey_1e)\|;
\end{aligned}$$

$$\begin{aligned}
&\eta_n(e,z,z_1,\dots,z_n,c_1,\dots,c_n,t_1,\dots,t_n) =\\
&\wedge_{i=1}^n\|c_i \in C\| \wedge \|eze = \sum_{i=1}^n c_iez_ie\|\\
&\wedge_{i=1}^n\|t_i \in C\| \wedge [(\wedge_{i=1}^n\|t_i = 0\|) \vee \|\sum_{i=1}^n t_iez_ie \neq 0\|];
\end{aligned}$$

$$\begin{aligned}
\theta_n(e) &= (\forall c)(\forall x_1)(\exists x_2)(\forall y_1)(\forall y_2)(\exists z_1)\dots(\exists z_n)(\forall z)\\
&\quad (\exists c_1)\dots(\exists c_n)\chi_0(e,x_1,x_2)\\
&\quad \wedge\chi_1(e,y_1,y_2) \wedge \chi_2(e,y_1,y_2)\\
&\quad \wedge\eta_n(e,z,z_1,\dots,z_n,c_1,\dots,c_n,t_1,\dots,t_n);\\
\Theta_n &= (\exists e)\theta_n(e) \qquad (6.2)
\end{aligned}$$

Clearly $e \in A$ is a faithful abelian idempotent of finite C-rank if and only if $A \models \theta_n(e)$ for some $n > 0$.

Lemma 6.3.7 *Let R be a semiprime ring, $A = RC$, $H = O(A)$, let $\psi \in Q_C{<}X{>}$ be a strict GPI of R and $0 \neq a \in A$. Then:*

(i) For all $P \in Spec(B)$ there exists a number $n = n(P)$, $n = k^2$, such that $\phi_P(H) \models \Theta_n$;

(ii) For all $P \in Spec(B)$ with $E(a) \notin P$ there exists a number $n = n(P)$ such that $\phi_P(H) \models (\exists x)(\exists e)(\theta_n(e) \wedge \|e = ax\|)$.

Proof. Let e be any minimal idempotent of $\overline{H}$ and let $n = \dim_{\overline{C}}(\Delta)$ where $\Delta = e\overline{H}e$. Clearly $n = k^2 < \infty$ and

$$\phi_P(H) \models \theta_n(e) \quad \text{and} \quad \phi_P(H) \models \Theta_n$$

which proves **(i)**.

Now let $E(a) \notin P$. Then $\bar{a} = \phi_P(a) \neq 0$ by Corollary 3.2.4. Therefore the right ideal $0 \neq \bar{a}\overline{H}$ of $\overline{H}$ contains a minimal idempotent of $\overline{H}$ and so $\phi_P(H) \models (\exists x)(\exists e)(\theta_n(e) \wedge \|e = ax\|)$.

It is well-known that any right (left) ideal of a centrally closed prime GPI ring contains a minimal idempotent e such that eRe is a finite-dimensional vector space over its center eC. We now prove the analogue of this result for semiprime rings.

Theorem 6.3.8 *Let R be a semiprime ring with extended centroid C, $Q = Q_{mr}(R)$, $A = RC \subseteq Q$ the central closure of R, and N a nonzero right (left) ideal of A. Suppose that $\phi \in Q_C{<}X{>}$ is a strict GPI on R. Then there is a central idempotent $u \in C$ and a uC-faithful abelian idempotent h' in A of finite uC-rank n.*

Proof. We set $H = O(A)$ and let $0 \neq a \in N$. Note that aH is an orthogonally complete subset of H by Lemma 3.1.18. Choose a maximal ideal P of B such that $\phi_P(a) \neq 0$ (i.e., $E(a) \notin P$). Then by Lemma 6.3.7**(ii)** $\phi_P(H) \models \Theta'_n$ for some natural number n where $\Theta'_n = (\exists x)(\exists h)(\theta_n(h) \wedge \|h = ax\|)$. According to Theorem 3.2.10, there exists a central idempotent $f \notin P$ such that $fH \models \Theta'_n$. Therefore there exists an abelian idempotent $h \in faH$ of finite fC-rank n such that $r_{fC}(h) = 0$. Pick a basis $z_1, z_2, \ldots, z_n \in hHh$ of the fC-module hHh. Note that $hHh = \oplus_{i=1}^n fCz_i$. By Proposition 3.1.14

$$h = \sum_{v \in V}{}^{\perp} h_v v \quad \text{and} \quad z_i = \sum_{v_i \in V_i}{}^{\perp} z_{v_i} v_i,$$

where V, V_i are dense orthogonal subsets of B and $h_v \in aA$, $z_{v_i} \in A$ for all $v \in V$, $v_i \in V_i$, $i = 1, 2, \ldots, n$. Pick idempotents $v \in V$, $v_1 \in V_1, \ldots, v_n \in V_n$ such that $u = fvv_1 \ldots v_n \neq 0$. Since $r_{fC}(h) = 0$, $h' = h_v u = hu \neq 0$. Clearly $h' \in aA$ is an idempotent and $z_i' = z_i u = z_{v_i} u \in h'Ah'$, $i = 1, 2, \ldots, n$. From $hHh = \oplus_{i=1}^{n} fCz_i$ we conclude that

$$h'Ah' \subseteq h'Hh' = uhHh = \sum_{i=1}^{n} Cuz_i = \sum_{i=1}^{n} Cz_i' \subseteq h'Ah'.$$

Therefore $h' \in aA \subseteq N$ is a nonzero abelian idempotent of finite uC-rank. The proof is complete.

The following decomposition theorem for semiprime rings will be especially useful for the determination of generators of the $\mathcal{T}$-ideal of GPI's in section 6.5.

Theorem 6.3.9 *Let R be a semiprime ring with extended centroid C, $Q = Q_{mr}(R)$ and H the orthogonal completion of the central closure $RC \subseteq Q$ of R. Suppose that R has a strict GPI $h(X) \in Q_C{<}X{>}$. Then there exist a natural number $t > 0$ and nonzero idempotents $u_1, u_3, \ldots, u_t \in H$ such that:*

(i) *The $E(u_i)$'s are an orthogonal set whose sum is 1;*

(ii) *u_i is a faithful abelian idempotent of finite rank $n_i = k_i^2$ of $E(u_i)C$-algebra $E(u_i)H$, $i = 1, 2, \ldots, t$;*

(iii) *If $M \in Spec(B)$ with $E(u_i) \notin M$ then $\phi_M(u_i Q u_i)$ is an n_i-dimensional division algebra over its center $\phi_M(u_i C)$;*

(iv) *$e = u_1 + u_2 + \ldots + u_t$ is a faithful abelian idempotent of the C-algebra H such that uHu is a finitely generated C-module.*

Proof. By Lemma 6.3.7(**i**) for every $P \in Spec(B)$ $\phi_P(H) \models \Theta_{n(P)}$ for some natural number $n(P) = k^2$. According to Theorem 3.2.18 (with H playing the role of R) there exists a family of pairwise orthogonal nonzero idempotents $\{f_1, f_2, \ldots, f_t\} \subseteq C$ and natural numbers $n_1, n_2, \ldots, n_t$ such that $f_1 + f_2 + \ldots + f_t = 1$

and $f_iH \models \Theta_{n_i}$, $i = 1, 2, \ldots, t$. Thus f_iH contains an f_iC-faithful abelian idempotent u_i of rank n_i over f_iC. Clearly $E(u_i) = f_i$ and so both **(i)** and **(ii)** have been proved. Now suppose $E(u_i) \notin M$. By Corollary 3.2.4 $\phi_M(u_i) \neq 0$. Setting $D = O(R)$ and $\overline{D} = \phi_M(D)$, we recall that $\overline{D}$ is a prime ring with extended centroid $\phi_M(C)$ and $\overline{D} \subseteq \phi_M(H) \subseteq Q_s(\overline{D})$. Therefore $\phi_M(H)$ is a prime ring. Since $\phi_M(u_i)$ is a nonzero idempotent, it follows that $\phi_M(u_i)\phi_M(H)\phi_M(u_i) = \phi_M(u_iHu_i)$ is a prime ring as well. Obviously a prime von Neumann regular ring all of whose idempotents are central is a division ring. Therefore $\phi_M(u_iHu_i)$ is a division ring. By Corollary 2.3.12 the center $Z(\phi_M(u_i)\phi_M(H)\phi_M(u_i))$ is equal to $\overline{C}\phi_M(u_i) = \phi_M(u_iC)$. Consider the following decomposition of the C-module H:

$$H = u_iHu_i \oplus (1-u_i)Hu_i \oplus u_iH(1-u_i) \oplus (1-u_i)H(1-u_i).$$

It follows that $(PH) \cap (u_iHu_i) = Pu_iHu_i$ and so $\ker(\phi_M) \cap (u_iHu_i) = Pu_iHu_i$. Choose a basis $z_1, z_2, \ldots, z_n$ of the C-module u_iHu_i, where $n = n_i$. Then $Pu_iHu_i = \oplus_{i=1}^{n} PCz_i$ and so $\phi_M(u_iHu_i) = \oplus_{i=1}^{n}\overline{C}\phi_M(z_i)$. Therefore $\dim_{\phi_M(u_iC)}(\phi_M(u_iHu_i)) = n_i$ and **(iii)** is proved. Finally it is an easy matter to see that $e = u_1 + u_2 + \ldots + u_t$ is a faithful abelian idempotent over C (in fact $eHe = \oplus_{i=1}^{t} u_iHu_i$) and that eHe is finitely generated over C (the number of generators being $\leq n_1n_2\ldots n_t$). The proof is complete.

Corollary 6.3.10 *Let R be a semiprime ring with extended centroid C, $B = B(C)$, $Q = Q_{mr}(R)$ and $D = O(R)$ the orthogonal completion of R and $H = O(RC)$. Then the following conditions are equivalent:*

(i) R has a strict GPI $\phi \in Q_C{<}X{>}$;

(ii) The orthogonal completion $O(RC)$ contains a faithful abelian idempotent e such that eHe is finitely generated over C;

(iii) For all $P \in Spec(B)$ the ring $\phi_P(D)$ is GPI;

(iv) For all $P \in Spec(B)$ the ring $\phi_P(H)$ is primitive with nonzero socle and the associated division ring is a finite dimensional over its center;

(v) For all $P \in Spec(B)$ the ring $\phi_P(Q)$ is primitive with nonzero socle and the associated division ring is a finite dimensional over its center.

Proof. The implication **(i)** $\Rightarrow$ **(iii)** is an immediate consequence of Lemma 6.3.7**(i)**. Since the proof of Theorem 6.3.9 only rested on the assumption that each $\phi_P(H)$ was *GPI*, it follows that **(iii)** implies **(ii)**. The equivalence of **(iii)**, **(iv)** and **(v)** follows from Corollary 6.1.7. Now we proceed to prove that **(ii)** $\Rightarrow$ **(i)**. Let $eO(RC)e$ be an n-generated C-module. It is clear that

$$St_{n+1}(ex_1e, \dots, ex_{n+1}e) = \sum_{\sigma \in S_{n+1}} \epsilon(\sigma) ex_{\sigma(1)}e \dots ex_{\sigma(n+1)}e$$

is a *GPI* on R. Since

$$\begin{aligned}&\Phi_P(St_{n+1}(ex_1e, \dots, ex_{n+1}e))\\ &= St_{n+1}(\phi_P(e)x_1\phi_P(e), \dots, \phi_P(e)x_{n+1}\phi_P(e)) \neq 0\end{aligned}$$

for all $P \in Spec(B)$, $St_{n+1}(ex_1e, \dots, ex_{n+1}e)$ is strict.

Theorem 6.3.11 *Let R be a semiprime ring with extended centroid C and $Q = Q_{mr}(R)$. Suppose that $\phi \in Q_C\langle X\rangle$ is a strict GPI on R. Then:*

(i) R is right and left nonsingular (i.e, $Z_r(R) = 0 = Z_l(R)$);

(ii) Q is a right selfinjective von Neumann regular ring with a faithful abelian idempotent e such that eQe is a finitely generated C-module.

Proof. **(i)** Since $O(RC) \subseteq Q_s(R)$, it is enough to show that the orthogonal completion H of the central closure $A = RC$ is right and left nonsingular (see Corollary 3.1.15, Lemma 2.1.13). According to Corollary 6.3.10, $\phi_P(H)$ is a primitive ring with nonzero socle for any maximal ideal P of $B = B(C)$. By Theorem 4.3.7**(iv)** the socle of a primitive ring belongs to any essential left (right) ideal. Hence $Z_l(\phi_P(H)) = 0 = Z_r(\phi_P(H))$. Then by Corollary 3.2.13

$$\phi_P(Z_l(H)) = 0 = \phi_P(Z_r(H))$$

for all $P \in Spec(B)$. It follows from Corollary 3.2.4 that H is left and right nonsingular.

(ii) First of all we note that Q is a centrally closed orthogonally complete ring by Theorem 2.1.11 and Proposition 3.1.10. According to Corollary 6.3.10, $\phi_P(Q)$ is a primitive ring with nonzero socle and the associated division ring is finite dimensional over its center. Since $Q_{mr}(Q) = Q$, it follows from Corollary 6.3.10 (with Q instead of R) that Q has a faithful abelian idempotent e such that eQe is a finitely generated C-module. In view of **(i)** the other properties of Q are given by Theorem 2.1.15. The proof is complete.

Our next aim is to show that Corollary 6.1.3 also holds for semiprime rings. To this end the following lemma will be useful.

Lemma 6.3.12 *Let R be a semiprime ring with extended centroid C, $Q = Q_{mr}(R)$ and $\phi(x) = \sum_{i=1}^{m} a_i x b_i \in Q_C\!<\!X\!>$. Suppose that $\sum_{i=1}^{m} Ca_i = \oplus_{i=1}^{m} Ca_i$ and $E(a_i) = E(b_i) \neq 0$ for all $i = 1, 2, \ldots, m$. Then ϕ is not a GPI on R.*

Proof. Suppose that ϕ is a *GPI* on R. By Theorem 2.3.3 there exist elements $u_1, \ldots, u_n, v_1, \ldots, v_n \in R$ such that

$$a = \sum_{j=1}^{n} u_j a_1 v_j \neq 0 \quad \text{but} \quad \sum_{j=1}^{n} u_j a_i v_j = 0 \quad \text{for} \quad i > 1.$$

Clearly $\sum_{j=1}^{n} u_j\phi(v_jx) = axb_1$ is a GPI on R. Therefore $aRb_1 = 0$ and so $aE(b_1) = 0$ by Lemma 2.3.10. Then

$$0 = aE(b_1) = \left(\sum_{j=1}^{n} u_ja_1v_j\right) E(b_1) = \sum_{j=1}^{n} u_j(E(b_1)a_1)v_j = a,$$

a contradiction.

Proposition 6.3.13 *Let R be a semiprime ring with extended centroid C and $Q = Q_{mr}(R)$. Suppose that $\phi(x) = \sum_{i=1}^{m} a_ixb_i \in Q_C{<}X{>}$ is a GPI on R. Then $\phi = 0$.*

Proof. Suppose that $\phi \neq 0$. Taking into account Theorem 2.3.9(**iv**), we can assume without loss of generality that

$$\sum_{i=1}^{m} Ca_i = \oplus_{i=1}^{m} Ca_i.$$

Replacing (if it is necessary) a_i and b_i by $E(b_i)a_i$ and $E(a_i)b_i$ we can assume also that $E(a_i) = E(b_i)$ for all $i = 1, 2, \dots, m$ (see Theorem 2.3.9(**ii**)). The conditions of Lemma 6.3.12 are now fulfilled, and by Lemma 6.3.12 a contradiction is reached.

Now we proceed to prove the analogs of the results of Section 6.2 for semiprime rings. We start with the following

Corollary 6.3.14 *Let R be a prime ring with extended centroid C and $Q = Q_{mr}(R)$, let U be an additive subgroup of R which is not GPI, and fix $x \in X$. Let $T_i = \{\phi_{ij}(x) \mid j = 1, 2, \dots, n_i\}$, $i = 1, 2, \dots, m$, be m given subsets of $Q_C{<}X{>}$ each of which is C-independent. Then there exists $u \in U$ such that for each $i = 1, 2, \dots, m$ the subset $T_i(u) = \{\phi_{ij}(u) \mid j = 1, 2, \dots, n_i\} \subseteq Q$ is C-independent.*

Proof. Exactly the same proof as that of Lemma 6.1.8 can be used, with Q_s now replaced by Q_{mr}.

Our next goal is to prove the analogue of Theorem 6.2.3 for semiprime rings. Let R be a semiprime ring with a (fixed) antiautomorphism g and $Q = Q_{mr}(R)$. The notions of g-substitution and g-identity $\phi \in Q_C{<}X{>}$ for semiprime rings are defined analogously to that of prime ring.

Lemma 6.3.15 *Let R be a prime ring with extended centroid C and $Q = Q_{mr}(R)$. Suppose that g is an antiautomorphism of R and*

$$0 \neq \phi(x) = \sum_{i=1}^{m} a_i x b_i + \sum_{j=1}^{n} c_j x^g d_j \in Q_C{<}X \cup X^g{>}$$

be such that $\dim_C(\phi(I)C) < \infty$ *for some* $0 \neq I \triangleleft R$. *Then R is GPI (in particular if ϕ is a g-identity on I then R is GPI).*

Proof. Suppose that R is not *GPI* and $n = 0$. Without loss of generality we can assume that $a_1, a_2, \ldots, a_m$ are C-independent. Multiplying by a suitable element r from the right we can assume also that $b_i \in R$. By Remark 6.3.1 there exist an element $r' \in R$ such that $a_1 r', a_2 r', \ldots, a_m r'$ are C-independent elements of R. Hence $\phi'(x) = \phi(r'x) \neq 0$. Since $\phi'(I)C = \phi(r'I)C \subseteq \phi(I)C$, we conclude that $\dim_C(\phi'(I)C) < \infty$ and so by Lemma 6.1.2 and Lemma 6.1.4 R is *GPI*, a contradiction. The general case is considered analogously to that of Lemma 6.2.1.

Now the proof of Theorem 6.2.3 yields the following

Corollary 6.3.16 *Let R be a prime ring with an antiautomorphism g and extended centroid C, $Q = Q_{mr}(R)$ and let $0 \neq \phi \in Q_C{<}X \cup X^g{>}$ be a g-identity on $0 \neq I \triangleleft R$. Then R is GPI.*

Lemma 6.3.17 *Let R be a semiprime ring with an antiautomorphism g and extended centroid C, $Q = Q_{mr}(R)$ and let*

$$0 \neq \phi = \phi(x_1, \dots, x_n, x_1^g, \dots, x_n^g) \in Q_C{<}X \cup X^g{>}$$

be a g-identity of R. Then there exists an ideal I of R such that $\phi(x_1, \dots, x_n, y_1, \dots, y_n)$ is a GPI on I and $e^g = e$ for all $e^2 = e \in (1 - E(I))C$.

Proof. First of all we recall that by Proposition 2.5.4 g can be uniquely extended to an antiautomorphism of $Q_s = Q_s(R)$. Clearly $C^g = C$. By Zorn's Lemma there exists an ideal I of R maximal with respect to the property that

$$\phi(x_1, \dots, x_n, y_1, \dots, y_n) \quad \text{is a } GPI \text{ on } \quad I.$$

Suppose that $u^g \neq u$ for some $u^2 = u \in (1 - E(I))C$. If $uu^{g^{-1}} = u = uu^g$, then

$$u^g = \left(uu^{g^{-1}}\right)^g = u^g u = u,$$

a contradiction. Therefore either $u \neq u^g u$, or $u \neq u^{g^{-1}}u$. In the first case we set $v = u(1 - u^g)$ and $w = u^{g^{-1}}(1 - u)$, otherwise we let $v = u\left(1 - u^{g^{-1}}\right)$ and $w = u^{g^{-1}}\left(1 - u^{g^{-2}}\right)$. Clearly $w^g = v$ and $vw = 0$. Hence $0 = (vw)^g = v^g v$ and

$$vw = 0 = v^g v \tag{6.3}$$

Let $J = v(v : R)_R$ and $K = w(w : R)_R$. Since $v = w^g$, $J = K^g$ as well. Obviously

$$\psi = \phi(vx_1 + wz_1, \dots, vx_n + wz_n, v^g x_1^g + vz_1^g, \dots, v^g x_n^g + vz_n^g)$$

vanishes under all substitutions $x_i \mapsto r_i \in J$, $z_i \mapsto s_i \in K$, $i = 1, 2, \dots, n$. We now infer from (6.3) that

$$v\psi = v\phi(x_1, \dots, x_n, z_1^g, \dots, z_n^g).$$

Recall that $vr = r$ for all $r \in J$ and $J^{g^{-1}} = K$. Pick any $r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_n \in J$. By the above results ψ vanishes under the substitution $x_i \mapsto r_i$, $z_i \mapsto s_i^{g^{-1}}$, $i = 1, 2, \ldots, n$. Therefore $\phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$ is a GPI on J. Recalling that $J = v(v : R)_R$ and $v \in (1 - E(I))C$, we note that $E(I)J = 0$ and so $IQJ = 0$. Therefore $I + J = I \oplus J$. Since $IQJ = 0$,

$$\begin{aligned}&\phi(a_1 + b_1, \ldots, a_n + b_n, c_1 + d_1, \ldots, c_n + d_n)\\ &= \phi(a_1, \ldots, a_n, c_1, \ldots, c_n) + \phi(b_1, \ldots, b_n, d_1, \ldots, d_n) = 0\end{aligned}$$

for all $a_i, c_i \in I$, $d_i, b_i \in J$, $1 \leq i \leq n$. It follows that $\phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$ is a GPI on $I + J$ in contradiction to the choice of I. Thus $u^g = u$ for all $u \in (1 - E(I))C$ and the proof is complete.

Theorem 6.3.18 *Let R be a semiprime ring with an antiautomorphism g and extended centroid C, $Q = Q_{mr}(R)$, $Q_s = Q_s(R)$ and let*

$$0 \neq \phi = \phi(x_1, \ldots, x_n, x_1^g, \ldots, x_n^g) \in Q_C{<}X \cup X^g{>}$$

be a strict g-identity of R. Then the ring R has a strict GPI $\psi \in Q_{sC}{<}X{>}$.

Proof. By Corollary 6.3.10 it is enough to show that $\phi_P(Q)$ is a primitive ring with nonzero socle and an associated division ring is finite dimensional over its center for all $P \in Spec(B)$ where $B = B(C)$. Let an ideal I of R be as in Lemma 6.3.17. Clearly $O(I)$ is an ideal of $D = O(R)$ and

$$\psi = \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

is a GPI on $O(I)$ (see Remark 3.1.8 and Remark 3.1.9). We also note that $r_C(\psi) = r_C(\phi) = 0$, $r_C(O(I)) = r_C(I)$ and so $E(O(I)) = E(I)$. We set $v = (1 - E(I))$ and $J = v(v : R)_R$.

Since $(v : R)_R$ is a dense ideal, $r_C(J) = r_C(v) = E(I)C$ and so $E(J) = v$. Let $P \in Spec(B)$. Then either $E(I) \notin P$ or $v \notin P$. Suppose that $E(I) \notin P$. Then by Corollary 3.2.4 $\phi_P(O(I))$ is a nonzero ideal with a nonzero GPI on a prime ring $\phi(D)$ and so $\phi_P(Q)$ has the desired properties (see Corollary 6.1.7). Consider now the case when $v \notin P$. Since $v = E(J) = E(O(J))$, we conclude that $\phi_P(O(J)) \neq 0$. According to Lemma 6.3.17, $u^g = u$ for all $u \in vC$. We infer from Remark 3.1.8, Remark 3.1.9 and Remark 3.1.16 that ϕ is a g-identity of $O(J)$. Further $P = (1-v)B + P \cap vB$ and so $P^g = P$. Hence g induces an antiautomorphism h of $\phi_P(D)$. We set $\overline{Q} = \phi_P(Q)$ and $\overline{C} = \phi_P(C)$. Consider the canonical extension $\Phi_P : Q_C{<}X \cup X^g{>} \rightarrow \overline{Q}_{\overline{C}}{<}X \cup X^h{>}$ of ϕ_P. Clearly $\Phi_P(\phi)$ is an h-identity on $0 \neq \phi_P(O(J)) \lhd \phi(D)$. By Lemma 6.3.15 $\phi_P(D)$ is GPI and so by Corollary 6.1.7 the ring $\overline{Q}$ has the desired properties. The proof is complete.

Remark 6.3.19 *Let R be a semiprime ring with extended centroid C and $Q = Q_{mr}(R)$. Further let K be a submodule of Q_R. Then $E(K) = E(K \cap R)$ and $r_R(K) = r_R(K \cap R) = r_R(E(K))$.*

Proof. We set $L = K \cap R$. Let $Lc = 0$ for some $c \in C$. Pick any $q \in K$ and set $I = (q : R)_R$. We note that I is a dense right ideal of R and $qI \subseteq L$. Hence $0 = qIc = (qc)I$ and so $qc = 0$ by Proposition 2.1.7. It follows that $r_C(L) = r_C(K)$ which implies $E(K) = E(L)$.

It follows from Lemma 2.3.10 that for any submodule $U \subseteq Q_R$ and element $r \in R$ the relation $Ur = 0$ is equivalent to $E(U)r = 0$. Applying what we just proved, we infer that $r_R(K) = r_R(K \cap R)$.

We close this section with the following useful result (here we call a ring R a PI-ring if it has a polynomial identity with integral coefficients at least one of which equals 1).

Theorem 6.3.20 *Let R be a semiprime ring with extended centroid C and $Q = Q_{mr}(R)$. Then the following conditions are equivalent:*

(i) R has a strict GPI belonging to $Q_C{<}X{>}$;

(ii) R contains a right (left) ideal L such that $r_R(L) = 0$ ($l_R(L) = 0$) and L is a PI-ring;

(iii) Any right (left) ideal K of R contains a right (left) ideal N such that $r_R(K) = r_R(N)$ ($l_R(K) = l_R(N)$) and N is a PI-ring.

Proof. **(i) ⇒ (ii)** We set $A = RC \subseteq Q$ and $H = O(A)$. By Theorem 6.3.9**(iv)** H contains a faithful abelian idempotent v (hence $E(v) = 1$) such that vHv is an n-generated C-module for some natural number n. Then $ST_{n+1}(v; X)$ is a strict GPI on H. Since $H \subseteq Q_s(R)$, it is enough to prove only the "right" version of **(ii)** and **(iii)** (see Proposition 3.1.10). We set $L = vH \cap R$ and claim that L is a PI-ring and $r_R(L) = 0$. Indeed, since $vx = x$ for all $x \in L$, $St_{n+1}(x_1, \ldots, x_{n+1})x_{n+2}$ is a polynomial identity of L. Further by Remark 6.3.19 $r_R(L) = r_R(vH)$. Let $r \in r_R(vH)$. Then $vHr = 0$ and so $r = E(v)r = 0$ by Lemma 2.3.10.

(ii) ⇒ (iii) Let K be a nonzero right ideal of R and $f = f(x_1, \ldots, x_m)$ a polynomial identity of L. Then $O(K)$ and $O(L)$ are right ideals of the orthogonal completion $O(R)$ of R. It follows from Remark 3.1.8 and Remark 3.1.9, that f is a polynomial identity on $O(L)$. By Proposition 3.1.11 there exist $k \in O(K)$, $l \in O(L)$ such that $E(k) = E(O(K))$ and $E(l) = E(O(L))$. According to Lemma 3.1.18 $kO(R)l$ is an orthogonally complete subset of $O(R)$ and so there exists $r \in O(R)$ such that $E(krl) = E(kO(R)l)$ by Proposition 3.1.11. For all $d_1, \ldots, d_{m+1} \in O(R)$ we have $ld_ikr \in O(L)$, $1 \le i \le m+1$, and so

$$f(krld_1, krld_2, \ldots, krld_m)krld_{m+1} =$$
$$krf(ld_1kr, ld_2kr, \ldots, ld_mkr)ld_{m+1} = 0.$$

Therefore the ring $krlO(R)$ satisfies the polynomial identity $f(x_1,\dots,x_n)x_{n+1}$. Setting $N = (krlO(R)) \cap K$, we claim that $r_R(N) = r_R(K)$. Indeed, let $Nr = 0$ for some $a \in R$. Since N is a right ideal, we have $NRa = 0$. By Lemma 2.3.10 we have that $E(a)N = 0$. Suppose that $E(a)krl \neq 0$. By Proposition 3.1.14 $k = \sum_{v \in V} k_v v$ where V is a dense orthogonal subset of $B = B(C)$ and $k_v \in K$ for all $v \in V$. Then $k_v(E(a)rl) = v(E(a)krl) \neq 0$ for some $v \in V$ (see Theorem 2.3.9(i)). Since $I = (rl : R)_R$ is a dense right ideal of R, $E(a)k_v rlI = k_v(E(a)rl)I \neq 0$. On the other hand $k_v rlI \subseteq N$ and so $E(a)k_v rlI = 0$, a contradiction. Therefore $E(a)krl = 0$. By the choice of r we then have $E(a)kO(R)l = 0$ and hence $E(a)kE(l) = 0$ by Lemma 2.3.10. By the choice of l we have $E(l) = E(L)$. Since $r_R(L) = 0$ and $L(1 - E(L))(E(L) : R)_R = 0$, it follows that $E(L) = 1$ and so $E(a)k = 0$. By the choice of k we then have that $KE(a) = 0$ and hence $Ka = 0$ by Lemma 2.3.10 which proves our claim.

(iii) $\Rightarrow$ (i) Taking $K = R$, we conclude that there exists a right ideal L of R such that $r_R(L) = 0$ and L is a PI-ring. Let $f = f(x_1,\dots,x_m)$ be a polynomial identity of L and let $l \in O(L)$ be as above. Without loss of generality we can assume that f is multilinear and the monomial $x_1x_2\dots x_m$ is involved in f with the coefficient 1. We claim that $\phi = f(lx_1, lx_2, \dots, lx_m)lx_{m+1}$ is a strict GPI on $O(R)$. Indeed, clearly ϕ is a GPI on R. Setting $e = 1 - E(L)$ and $I = (e : R)_R$, we see that $0 = LeI$ and $eI \subseteq R$. Hence $eI = 0$ and $E(L) = E(l) = 1$. Suppose $c\phi = 0$ for some $c \in C$. Then $clx_1lx_2\dots lx_{m+1} = 0$. Recall that the C-module $Qx_1Qx_2\dots Qx_{m+1}Q$ is isomorphic to the $(m+2)$-fold tensor product $Q\otimes_C Q\dots\otimes_C Q$ via the mapping given by the rule $q_1x_1q_2\dots x_{m+1}q_{m+1} \mapsto q_1 \otimes q_2 \otimes \dots \otimes q_{m+2}$ and its consequences. Since $Cl \cong C$, Cl is an injective C-module and so Cl is a direct summand of the C-module Q. Therefore the C-submodule $C(l\otimes l \otimes \dots \otimes l \otimes 1)$ is isomorphic to $C \otimes_C C \otimes_C \dots \otimes_C C \cong C$ and hence $r_C(lx_1lx_2\dots lx_{m+1}) = 0$. The proof is complete.

Semiprime rings with GPI were investigated by K. I. Beidar in [21], [22], [24] and [27] where Theorem 6.3.8, Theorem 6.3.11 and Proposition 6.3.13 were proved. The proofs presented here are new. Besides the method of orthogonal completions, we have used here some ideas from [81]. The prime ring case of Theorem 6.3.20 was proved in S. K. Jain [135] and extended to semiprime rings in [27].

6.4 Lifting of GPI's

Our aim in this section is to prove the following theorem.

Theorem 6.4.1 *Let R be a semiprime ring with extended centroid C and $Q = Q_{mr}(R)$. Then any GPI $\psi = \psi(x_1, \dots, x_n) \in Q_C{<}X{>}$ on R is a GPI on Q.*

We start with the following useful

Proposition 6.4.2 *Let R be a prime ring with extended centroid C and $Q = Q_{mr}(R)$. Suppose that $0 \neq \phi \in Q_C{<}X{>}$ is a GPI on $0 \neq K \lhd R$ and $|C| < \infty$. Then R is a primitive ring with nonzero socle and a nonzero idempotent e such that $eRe = eC$.*

Proof. Obviously $I = (\cap_{c \in C}(c : R)_R) \cap K$ is a nonzero ideal of R and $IC = I$. Recalling that $Q_{mr}(I) = Q$, we conclude that C is the extended centroid of I and so I is centrally closed (see Lemma 2.1.9). Since ϕ is a nonzero GPI on I, we infer from Corollary 6.3.3 that $I = IC$ has a nonzero idempotent e such that eIe is a finite dimensional division C-algebra. Therefore eIe is a finite division ring. By Wedderburn's theorem on finite division rings eIe is a field (see Theorem 4.2.3). According to Corollary 2.3.12, the center $Z(eIe)$ is equal to eC and so $eIe = eC$. Since I is an ideal of R and $e \in I$, $eIe \subseteq eRe = e(eRe)e \subseteq eIe$ and so $eRe = eIe = eC$. Applying Proposition 4.3.3, we conclude that R is a primitive ring with nonzero socle. The proof is thereby complete.

Let R be a prime ring with extended centroid C and $Q = Q_{mr}(R)$. We fix a C-basis $\mathcal{A}$ containing 1 and consider the corresponding monomial basis $\mathcal{M}(\mathcal{A})$ of $Q_C\langle X\rangle$ determined by $\mathcal{A}$. Any element $\phi \in Q_C\langle X\rangle$ may be written $\phi = \sum_M \alpha_M M \in Q_C\langle X \cup X^g\rangle$, where $M \in \mathcal{M}(\mathcal{A})$ and $0 \neq \alpha_M \in C$. We refer the reader to the linearization process described in section 6.1 and section 6.2, in which various notions of degree, g-degree, height, g-height, and homogeneity are defined. Here we recall that ϕ is multilinear if and only if it is homogeneous of zero height.

Lemma 6.4.3 *Let R be a prime ring with extended centroid C and $Q = Q_{mr}(R)$. Suppose that*

$$0 \neq \phi = \phi(x_1, x_2, \dots, x_n) \in Q_C\langle X\rangle$$

is a GPI on $0 \neq K \lhd R$. Then ϕ is a GPI on the socle $Soc(A)$ of $A = RC$.

Proof. By Corollary 6.3.3 A is primitive with $Soc(A) \neq 0$. Replacing (if it is necessary) K by $K \cap Soc(A)$, we can suppose that $K \subseteq Soc(A)$. It follows from Theorem 4.3.7(**iv**) that $KC = Soc(A)$. In a view of Proposition 6.4.2 without loss of generality we can assume that $|C| = \infty$. Let $\phi = \sum_M \alpha_M M$ where $M \in \mathcal{M}(\mathcal{A})$ and $0 \neq \alpha_M \in C$. Further let $\deg_{x_1}(\phi) = m$. For every $0 \leq k \leq m$ we set

$$\phi_k = \sum_M \{\alpha_M M \mid \deg_{x_1}(M) = k\}.$$

Pick $m+1$ distinct elements $c_1, c_2, \dots, c_{m+1} \in C$. Clearly there exists a nonzero ideal $I \subseteq K$ of R such that $c_t I \subseteq R$ for all $t = 1, 2, \dots, m+1$. For any $1 \leq t \leq m+1$, $r_1 \in I$ and $r_2, r_3, \dots, r_n \in K$ we have

$$0 = \phi(c_t r_1, r_2, \dots, r_n) = \sum_{k=0}^{m} c_t^k \phi_k(r_1, r_2, \dots, r_n).$$

Using a Vandermonde determinant argument, we conclude that $\phi_k(r_1, r_2, \dots, r_n) = 0$ for all $k = 0, 1, \dots, m$. Continuing in this fashion we find a nonzero ideal J of R such that all homogeneous components ϕ_τ of ϕ are GPI's on J. It is enough to show that every ϕ_τ is an identity on $Soc(A)$. Therefore without loss of generality we can assume that ϕ is τ-homogeneous where $\tau = (k_1, k_2, \dots, k_n)$.

We proceed by induction on $ht(\phi)$. If $ht(\phi) = 0$, then ϕ is multilinear and so ϕ is an identity on JC. Further, JC is an ideal of A. By Theorem 4.3.7 $Soc(A) \subseteq JC$ (in fact $Soc(A) = JC$) and hence ϕ is an identity on $Soc(A)$. Suppose now that $ht(\phi) = m$ and our statement is proved for GPI's of height less then m. Notationally suppressing all variables in ϕ other than $x \in \{x_1, x_2, \dots, x_n\}$ (where $ht_x(\phi) > 0$) and picking a new variable $y \in X$ which does not appear in ϕ we form the element

$$\psi(x, y) = \phi(x + y) - \phi(x) - \phi(y)$$

and note the following properties of ψ:

$$\begin{aligned} &ht_x(\psi) < \deg_x(\phi) - 1 = ht_x(\phi); \\ &ht(\psi) < ht(\phi); \\ &\psi \quad \text{is a} \quad GPI \quad \text{on} \quad J. \end{aligned}$$

By the induction assumption every homogeneous component of ψ (and hence ψ itself) is a GPI on $Soc(A)$. Therefore

$$0 = \psi(r, s) = \phi(r + s) - \phi(r) - \phi(s)$$

for all $r, s \in Soc(A)$ and so ϕ is additive in every variable x_i on $Soc(A)$. Let

$$a_i = \sum_j c_{ij} r_{ij} \in Soc(A) \subseteq JC$$

where $c_{ij} \in C$, $r_{ij} \in J$. Then we have

$$\phi(a_1, \dots, a_n) = \sum_{j_1, \dots, j_n} c_{1j_1}^{k_1} \dots c_{nj_n}^{k_n} \phi(r_{1j_1}, \dots, r_{nj_n}) = 0$$

and hence ϕ is an identity on $Soc(A)$. The proof is complete.

Theorem 6.4.4 *Let R be a prime ring with extended centroid C and $Q = Q_{mr}(R)$. Suppose that*

$$0 \neq \phi = \phi(x_1, x_2, \ldots, x_n) \in Q_C{<}X{>}$$

is a GPI on $0 \neq K \lhd R$. Then ϕ is a GPI on Q.

Proof. Letting A denote the central closure RC of R, we infer from Corollary 6.3.3 and Lemma 6.4.3 that $Soc(A) \neq 0$ and ϕ is an identity on $Soc(A)$. Pick a nonzero idempotent $e \in Soc(A)$ such that Ae is a minimal left ideal of A. By Theorem 4.3.7 $Q = End(Ae_\Delta)$ where $\Delta = eAe$ is a division ring. Furthermore

$$QSoc(A) = QAeA = AeA = Soc(Q).$$

Suppose that ϕ is not a GPI on Q. Then there exist elements $q_1, q_2, \ldots, q_n \in Q$ and $a \in Ae$ such that

$$\phi(q_1, q_2, \ldots, q_n)a \neq 0. \tag{6.4}$$

Let $m = \deg(\phi) + 2$ and $\phi = \sum_M \alpha_M M$ where $M \in \mathcal{M}(\mathcal{A})$ and $0 \neq \alpha_M \in C$. Denote by T' the set of all coefficients appearing in ϕ and set $T'' = T' \cup \{q_1, \ldots, q_n\}$. Further let T be the set of all m-fold products of elements from T''. Obviously T', T'' and T all are finite. By Litoff's theorem there exists an idempotent $v \in Soc(A)$ such that $vta = ta$ for all $t \in T$. Consider now any monomial

$$M = a_{i_0} x_{j_1} a_{i_1} \ldots x_{j_k} a_{i_k}$$

appearing in ϕ where $0 \neq a_{i_s} \in Q$, $x_{j_r} \in X$. We claim that

$$\begin{aligned} &a_{i_0} v q_{j_1} v \ldots v q_{j_r} v a_{i_r} q_{j_{r+1}} \ldots q_{j_k} a_{i_k} a = \\ &a_{i_0} q_{j_1} \ldots q_{j_r} a_{i_r} q_{j_{r+1}} \ldots q_{j_k} a_{i_k} a \end{aligned} \tag{6.5}$$

for all $r = 1, 2, \ldots, k$. Indeed, letting

$$t_1 = a_{i_r} q_{j_{r+1}} \ldots q_{j_k} a_{i_k} \quad \text{and} \quad t_2 = q_{j_r} t_1,$$

we note that $vt_1 a = t_1 a$ and $vt_2 a = t_2 a$ by the choice of v. Hence

$$a_{i_0} v q_{j_1} v \ldots v q_{j_r} v a_{i_r} q_{j_{r+1}} \ldots q_{j_k} a_{i_k} a =$$
$$a_{i_0} q_{j_1} \ldots v q_{j_{r-1}} v a_{i_{r-1}} q_{j_r} a_{i_r} \ldots q_{j_k} a_{i_k} a$$

which proves our claim. Since $vq_i v \in Soc(A)$ and ϕ is an identity on $Soc(A)$, it follows from (6.5) that

$$\phi(q_1, q_2, \ldots, q_n)a = \phi(vq_1v, vq_2v, \ldots, vq_nv)a = 0,$$

a contradiction to (6.4). The proof is thereby complete.

Proof of Theorem 6.4.1. Let $q_1, q_2, \ldots, q_n \in Q$. We set $q = \psi(q_1, \ldots, q_n)$ and $B = B(C)$. It is enough to prove that $\phi_P(q) = 0$ for all $P \in Spec(B)$ where $\phi_P : Q \to \overline{Q} = Q/PQ$ is the canonical projection of rings (see Corollary 3.2.4). We set

$$D = O(R),\ \overline{D} = \phi_P(D) \quad \text{and} \quad \overline{C} = \phi_P(C).$$

Letting Φ_P denote the canonical extension of ϕ_P to a homomorphism $Q_C{<}X{>} \to \overline{Q}_{\overline{C}}{<}X{>}$, we note that if $\overline{\psi} = \Phi_P(\psi) = 0$, then

$$\phi_P(q) = \overline{\psi}(\phi_P(q_1), \ldots, \phi_P(q_n)) = 0$$

as well. If $\overline{\psi} \neq 0$, then it is a nonzero GPI on $\overline{D}$ by Corollary 6.3.6 and by Theorem 6.4.4 we have

$$\phi_P(q) = \overline{\psi}(\phi_P(q_1), \ldots, \phi_P(q_n)) = 0.$$

Thus $\phi_P(q) = 0$ for all $P \in Spec(B)$ and the proof is thereby complete.

Now we proceed to prove the analogous result for g-identities of a semiprime ring where g is an antiautomorphism. Let R be a semiprime ring with extended centroid C and a fixed antiautomorphism g. We set $Q = Q_{mr}(R)$ and $Q_s = Q_s(R)$. The notions of g-substitution, g-identity $\phi \in Q_C{<}X \cup X^g{>}$ and g-degree are introduced analogously to that of prime rings (see section 6.2) and we leave the straightforward details for the reader. Let

$$\phi = \phi(x_1, \dots, x_n, x_1^g, \dots, x_n^g) = \sum_M \alpha_M M \in Q_C{<}X \cup X^g{>}$$
$$\text{where} \quad M \in \mathcal{M}(\mathcal{A}) \quad \text{and} \quad 0 \neq \alpha_M \in C$$

be a g-polynomial, $\tau = (m_1, \dots, m_n)$ and $\sigma = (m_1, \dots, m_{2n})$ sequences of natural numbers. We set

$$\begin{aligned} \phi_\tau &= \sum \{\alpha_M M \mid g\text{-}\deg_{x_i}(M) = m_i \text{ for all } \quad 1 \leq i \leq n\}; \\ \phi_\sigma &= \sum \{\alpha_M M \mid \deg_{x_i}(M) = m_i, \ \deg_{x_i^g}(M) = m_{n+i} \\ &\qquad \text{for all } \quad 1 \leq i \leq n\}. \end{aligned}$$

We will call ϕ_τ a g-homogeneous component of ϕ . Clearly ϕ_σ is a homogeneous component of ϕ. Here we note that ϕ is g-multilinear if and only if it is g-homogeneous of zero g-height.

Lemma 6.4.5 *Let R be a prime ring with extended centroid C, an antiautomorphism g and $Q = Q_{mr}(R)$. Suppose that*

$$0 \neq \phi = \phi(x_1, \dots, x_n, x_1^g, \dots, x_n^g) \in Q_C{<}X \cup X^g{>}$$

is a g-identity on $0 \neq K \lhd R$. Then ϕ is a g-identity on the socle $Soc(A)$ of $A = RC$.

Proof. First of all we note that g can be uniquely extended to an antiautomorphism of the ring $Q_s(R) \supseteq A$ by Proposition 2.5.4 (which we again denote by g). Secondly replacing (if it is necessary) K by $K \cap Soc(A)$, we can suppose that $K \subseteq Soc(A)$. It follows from Theorem 4.3.7 that $KC = Soc(A)$.

Suppose now that

$$\begin{aligned}&\phi(r_1,\dots,r_n,r_1^g,\dots,r_n^g)=0\\&\text{for all}\quad r_1,\dots,r_t\in Soc(A),\ r_{t+1},\dots,r_n\in K\end{aligned}$$

where $t\geq 0$ is given. We claim that

$$\begin{aligned}&\phi(r_1,\dots,r_n,r_1^g,\dots,r_n^g)=0\\&\text{for all}\quad r_1,\dots,r_{t+1}\in Soc(A),\ r_{t+2},\dots,r_n\in K.\end{aligned}\qquad(6.6)$$

We proceed by induction on $g\text{-}ht(\phi)$. If it is equal to 0, then any monomial appearing in ϕ is g-multilinear. Substituting zero instead of some variables (if it is necessary), we conclude that ϕ is a sum of g-multilinear identities on K. Therefore without loss of generality we can assume that ϕ is g-multilinear. If $g|_C=id_C$, then ϕ is a g-identity on $KC\supseteq Soc(R)$. Otherwise $a^g\neq a$ for some $a\in C$. Clearly $aJ\subseteq K$ for some nonzero ideal $J\subseteq K$ of R. Since ϕ is g-multilinear,

$$\begin{aligned}\phi &= \phi'(x_1,\dots,x_n,x_1^g,\dots,x_t^g,x_{t+2}^g,\dots,x_n^g)\\&\quad+\phi''(x_1,\dots,x_t,x_{t+2},\dots,x_n,x_1^g,\dots,x_n^g).\end{aligned}$$

Now for all $b\in J$, $r_1,\dots,r_t\in Soc(A)$ and $r_{t+2},\dots,r_n\in K$ we have

$$\begin{aligned}0 &= \phi'(r_1,\dots,r_t,b,r_{t+2},\dots,r_n,r_1^g,\dots,r_t^g,r_{t+2}^g,\dots,r_n^g)\\&\quad+\phi''(r_1,\dots,r_t,r_{t+2},\dots,r_n,r_1^g,\dots,r_t^g,b^g,r_{t+2}^g\dots,r_n^g);\\0 &= a\phi'(r_1,\dots,r_t,b,r_{t+2},\dots,r_n,r_1^g,\dots,r_t^g,r_{t+2}^g,\dots,r_n^g)\\&\quad+a^g\phi''(r_1,\dots,r_t,r_{t+2},\dots,r_n,r_1^g,\dots,r_t^g,b^g,r_{t+2}^g\dots,r_n^g).\end{aligned}$$

Since $a^g\neq a$, we conclude that

$$\begin{aligned}\phi'(r_1,\dots,r_t,b,r_{t+2},\dots,r_n,r_1^g,\dots,r_t^g,r_{t+2}^g,\dots,r_n^g) &= 0\quad\text{and}\\\phi''(r_1,\dots,r_t,r_{t+2},\dots,r_n,r_1^g,\dots,r_t^g,b^g,r_{t+2}^g\dots,r_n^g) &= 0.\end{aligned}$$

Consider now

$$\psi'(x) = \phi'(r_1, \ldots, r_t, x, r_{t+2}, \ldots, r_n, r_1^g, \ldots, r_n^g)$$

and

$$\psi''(y) = \phi''(r_1, \ldots, r_n, r_1^g, \ldots, r_t^g, y, r_{t+2}^g, \ldots, r_n^g).$$

By the above result they are generalized polynomial identities on J and $J^{g^{-1}}$ respectively. According to corollary 6.1.3, we have $\psi' = 0 = \psi''$. Therefore our claim is true for g-identities of zero g-height.

Suppose now that our claim is proved for g-identities of g-height less then $g\text{-}ht(\phi)$. Assume $\phi(r_1, \ldots, r_n, r_1^g, \ldots, r_n^g) \neq 0$ for some $r_1, \ldots, r_{t+1} \in Soc(A)$, $r_{t+2}, \ldots, r_n \in K$. We set

$$\psi(x, x^g) = \phi(r_1, \ldots, r_t, x, r_{t+2}, \ldots, r_n, r_1^g, \ldots, r_t^g, x^g, r_{t+2}^g, \ldots, r_n^g).$$

Clearly ψ is a nonzero g-identity on K and $g\text{-}ht(\psi) \leq g\text{-}ht(\phi)$. Let $g\text{-}\deg_x(\phi) = m$ and $\psi = \sum_M \alpha_M M$ where $M \in \mathcal{M}(\mathcal{A})$, $0 \neq \alpha_M \in C$. For every $0 \leq k, l \leq m$ with $k + l \leq m$ we set

$$\begin{aligned} \psi_{kl} &= \sum\{\alpha_M M \mid \deg_x(M) = k \quad \text{and} \quad \deg_{x^g}(M) = l\}; \\ \|\psi\| &= |\{(k,l) \mid \phi_{kl} \neq 0\}|. \end{aligned}$$

Since $\psi(r_{t+1}, r_{t+1}^g) = \phi(r_1, \ldots, r_n, r_1^g, \ldots, r_n^g) \neq 0$, ψ is not a g-identity on $Soc(A)$. Consider the set $\mathcal{T}$ of all nonzero g-identities $\tau(x, x^g)$ on $0 \neq J_\tau \triangleleft R$ having the properties τ is not a g-identity on $Soc(A)$ and $g\text{-}ht(\tau) \leq g\text{-}ht(\phi)$. Clearly $\psi \in \mathcal{T}$ and so $\mathcal{T} \neq \emptyset$. Pick $\tau \in \mathcal{T}$ with a minimal possible value of $\|\tau\|$. Without loss of generality we can assume that $N = J_\tau \subseteq Soc(A)$. Pick any pair of natural numbers s, t such that $\tau_{st} \neq 0$. Let $c \in C$. Clearly $cL \subseteq N$ for some nonzero ideal $L \subseteq N$ of R. Then for all $b \in L$ we have

$$\begin{aligned} 0 &= \sum_{kl} \tau_{kl}(b, b^g), \\ 0 &= \sum_{kl} c^k \left(c^g\right)^l \tau_{kl}(b, b^g). \end{aligned}$$

Setting

$$\beta(x, x^g) = \sum_{kl} \left(c^k \left(c^g\right)^l - c^s \left(c^g\right)^t\right) \tau_{kl}(x, x^g),$$

we conclude that β is a g-identity on L and $\|\beta\| < \|\tau\|$. Hence β is a g-identity on $Soc(A)$. In particular $\beta(a, a^g) = 0$ for all $a \in N$. Now it follows that

$$\begin{aligned} \tau(ca, c^g a^g) &= \sum_{kl} c^k \left(c^g\right)^l \tau_{kl}(a, a^g) \\ &= c^s \left(c^g\right)^t \sum_{kl} \tau_{kl}(a, a^g) \\ &= c^s \left(c^g\right)^t \tau(a, a^g) = 0. \end{aligned} \tag{6.7}$$

We consider

$$\chi(x, y, x^g, y^g) = \tau(x + y, x^g + y^g) - \tau(x, x^g) - \tau(y, y^g).$$

Clearly χ is a g-identity on N and

$$g\text{-}ht(\chi) < g\text{-}ht(\tau) < g\text{-}ht(\phi).$$

By induction assumption we then have that χ is a g-identity on $Soc(A)$. Therefore

$$0 = \chi(r, s, r^g, s^g) = \tau(r + s, r^g + s^g) - \tau(r, r^g) - \tau(s, s^g)$$

for all $r, s \in Soc(A)$. Let

$$a = \sum_j c_j r_j \in Soc(A) = NC$$

where $c_j \in C$, $r_j \in N$. Then by (6.7) we have

$$\tau(a, a^g) = \sum_j \tau(c_j r_j, c_j^g r_j^g) = 0$$

and hence τ is an identity on $Soc(A)$, a contradiction. The claim is thereby proved. From (6.6) it follows immediately that ϕ is a g-identity on $Soc(A)$. The proof is complete.

Theorem 6.4.6 *Let R be a prime ring with extended centroid C, an antiautomorphism g and $Q = Q_{mr}(R)$. Suppose that*

$$0 \neq \phi = \phi(x_1, \dots, x_n, x_1^g, \dots, x_n^g) \in Q_C{<}X \cup X^g{>}$$

is a g-identity on $0 \neq K \lhd R$. Then ϕ is a g-identity of $Q_s = Q_s(R)$.

Proof. As we know g can be uniquely extended to an antiautomorphism of the ring $Q_s(R)$ by Proposition 2.5.4 and we denote the extension again by g. Letting A denote the central closure RC of R, we infer from Corollary 6.3.3 and Lemma 6.4.5 that $Soc(A) \neq 0$ and ϕ is a g-identity on $Soc(A)$. Pick a nonzero idempotent $e \in Soc(A)$ such that Ae is a minimal left ideal of A. According to Theorem 4.3.7 $Q = End(Ae_\Delta)$, where $\Delta = eAe$ is a division ring, and

$$QSoc(A) = QAeA = AeA = Soc(Q).$$

Suppose that ϕ is not an identity on Q_s. Then there exist elements $q_1, q_2, \dots, q_n \in Q_s$ and $a \in Ae$ such that

$$\phi(q_1, \dots, q_n, q_1^g, \dots, q_n^g)a \neq 0. \tag{6.8}$$

We set $m = g\text{-deg}(\phi) + 2$. Let $\phi = \sum_M \alpha_M M$ where $M \in \mathcal{M}(\mathcal{A})$ and $0 \neq \alpha_M \in C$. Denote by T' the set of all coefficients appearing in ϕ and set $T'' = T' \cup \{q_1, \dots, q_n, q_1^g, \dots, q_n^g\}$. Further let T be the set of all m-fold products of elements from T''. Obviously T', T'' and T all are finite. By Litoff's theorem there exists an idempotent $v \in Soc(A)$ such that $vta = ta$ and $(ta)^{g^{-1}}v = (ta)^{g^{-1}}$ for all $t \in T$. Applying g to the last equality we infer that $v^g ta = ta$ for all $t \in T$. Hence

$$vta = ta = v^g ta \quad \text{for all} \quad t \in T.$$

At this point we note that the rest of proof is analogous to that of Theorem 6.4.4. In particular, making use of Lemma 6.4.5, we infer that

$$\phi(q_1,\dots,q_n^g)a = \phi(vq_1v,\dots,v^gq_n^gv^g)a = 0,$$

a contradiction. The proof is thereby complete.

Theorem 6.4.7 *Let R be a semiprime ring with extended centroid C, an antiautomorphism g and $Q = Q_{mr}(R)$. Then any g-identity*

$$\psi = \psi(x_1,\dots,x_n,x_1^g,\dots,x_n^g) \in Q_C{<}X \cup X^g{>}$$

is a g-identity of $Q_s = Q_s(R)$.

Proof. The proof is similar to that of Theorem 6.4.1. Pick $q_1,q_2,\dots,q_n \in Q_s$ and set $q = \psi(q_1,\dots,q_n,q_1^g,\dots,q_n^g)$. It is enough to prove that $q = 0$. By Lemma 6.3.17 there exists an ideal I of R such that $\phi = \psi(x_1,\dots,x_n,y_1,\dots,y_n)$ is a GPI on I and $e^g = e$ for all $e^2 = e \in (1 - E(I))C$. By Theorem 6.4.1 $E(I)\phi$ is a GPI on $Q_{mr}(I) = E(I)Q$. In particular $E(I)q = 0$. We set $e = 1 - E(I)$ and $J = e(e : R)_R$. It is enough to prove $eq = 0$. Clearly $Q_s(J) = eQ_s$ and

$$eq = \psi(eq_1,\dots,eq_n,(eq_1)^g,\dots,(eq_n)^g).$$

Hence without loss of generality we can assume that $I = 0$, $e = 1$ and $v^g = v$ for all $v^2 = v \in C$.

It is enough to prove that $\phi_P(q) = 0$ for all $P \in Spec(B)$ where $B = B(C)$ and $\phi_P : Q \to \overline{Q} = Q/PQ$ is the canonical projection of rings (see Corollary 3.2.4). Since $P^g = P$, g induces an antiautomorphism of Q_s/PQ_s which we denote again by g for simplicity. We set

$$D = O(R),\ \overline{D} = \phi_P(D),\ \overline{Q_s} = \phi_P(Q_s) \quad\text{and}\quad \overline{C} = \phi_P(C).$$

Letting Φ_P denote the canonical extension of ϕ_P to a homomorphism $Q_C{<}X \cup X^g{>} \to \overline{Q}_{\overline{C}}{<}X \cup X^g{>}$, we note that if

$\overline{\psi} = \Phi_P(\psi) = 0$, then $\phi_P(q) = 0$ as well. If $\overline{\psi} \neq 0$, then it is a nonzero g-identity of $\overline{D}$ as it was shown in the proof of Theorem 6.3.18. In the last case $\overline{\psi}$ is a g-identity of $Q_s(\overline{D}) \supseteq \overline{Q_s}$ by Theorem 6.4.6 and so $\phi_P(q) = 0$. Thus $\phi_P(q) = 0$ for all $P \in Spec(B)$ which completes the proof.

In [209] W. S. Martindale proved that every multilinear polynomial identity of a semiprime ring is an identity of its maximal right ring of quotients. Theorem 6.4.1 is a generalizarion of this result and it was proved by K. I. Beidar in [24]. Since the original proof used the existence of a central polynomial of a prime *PI*-ring, we used here the proof given in [81] for the prime ring case. The involution case of Theorem 6.4.7 was proved by K. I. Beidar, A. V. Mikhalev and K. Salavova in [37] (see also [36]) and here we used some ideas from their proof.

6.5 The $\mathcal{T}$-ideal of *GPI*'s

The aim of this section is to describe the $\mathcal{T}$-ideal of generalized polynomial identities of prime and semiprime rings. The results we present are due to K.I.Beidar (except Proposition 6.5.5 which is due to Littlewood [194]). Although there are considerable technical and notational aspects as well as case-by-case arguments involved in the proof, the end products are quite definitive and simply stated. The main results for centrally closed prime *GPI* rings (Theorem 6.5.7 and Theorem 6.5.12) show that the $\mathcal{T}$-ideal of all *GPI*'s has a single "obvious" generator, and for semiprime rings the finite generation of the $\mathcal{T}$-ideal of all *GPI*'s depends solely on the boundedness of the orders of the extended centroids of the Pierce stalks.

Let R be a semiprime ring with extended centroid C, $Q = Q_{mr}(R)$ and $RC \subseteq H \subseteq Q$ a C-subalgebra. Consider the ring $A = H_C{<}X{>}$. An endomorphism $\tau : A \to A$ is said to be an *H-endomorphism* if $h^\tau = h$ for all $h \in H \subseteq A$. An ideal

I of A is called a *$\mathcal{T}$-ideal* if it is an ideal of A and $I^\tau \subseteq I$ for any H-endomorphism $\tau : A \to A$. The last condition is equivalent to the following one: $f(g_1, g_2, \ldots, g_n) \in I$ for every $f(x_1, x_2, \ldots, x_n) \in I$ and all $g_1, g_2, \ldots, g_n \in A$ (i.e., I is closed under all substitutions). Obviously the set of all GPI's on R forms a $\mathcal{T}$-ideal which we shall denote by $\mathcal{G}(H;\, R)$. We also note that sums and intersections of $\mathcal{T}$-ideals are again $\mathcal{T}$-ideals. Given a subset $L \subseteq H_C{<}X{>}$, the intersection of all $\mathcal{T}$-ideals of $H_C{<}X{>}$ containing L is said to be the $\mathcal{T}$-ideal of $H_C{<}X{>}$ generated by L. We shall denote it by $\mathcal{T}(H;\, L)$ or simply $\mathcal{T}(L)$ when the context is clear. Here we note that $\mathcal{T}(L)$ is just the ideal of A generated by all $f(g_1, g_2, \ldots, g_n)$ where $f(x_1, \ldots, x_n) \in L$ and $g_1, \ldots, g_n \in A$.

Now let R be a primitive centrally closed algebra over a field C with minimal idempotent e such that $eRe = eC$. Given any natural number $q > 0$ we set

$$ST_2(e;\, X) = ex_1ex_2e - ex_2ex_1e, \quad \text{and} \quad L_q(e;\, X) = (ex_1e)^q - ex_1e.$$

Clearly $ST_2(e;\, X)$ is a GPI on R. Further if $|C| = q$, then $L_q(e;\, X)$ is a GPI on R as well.

The polynomial ring $K = C[x_1, x_2, \ldots, x_n]$ will play an important role in the sequel. In particular in case $q = |C| < \infty$ we will need the following well-known result (Remark 6.5.1). For any monomial $M = x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$ we set $M^\rho = x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ where $0 \le m_i < q$, $t_i \equiv m_i \, mod\,(q-1)$ and $m_i = 0$ if and only if $t_i = 0$, $i = 1, 2, \ldots, n$. Extending ρ by linearity to $K \to K$, we denote the resulting map again by ρ. A polynomial $f \in K$ is said to be *reduced* if $f^\rho = f$.

Remark 6.5.1 *Let $f \in C[x_1, x_2, \ldots, x_n]$ where $q = |C| < \infty$. Then:*

(i) f and f^ρ determine the same functions on C^n;

(ii) f vanishes on C^n if and only if $f^\rho = 0$;

Proof. The first statement easily follows from the obvious fact that $a^q = a$ for all $a \in C$.

Clearly it is enough to prove that a nonzero reduced polynomial g determines a nonzero function on C^n. We proceed by induction on n. If $n = 1$, then $\deg(g) \leq q - 1$. Hence g has at most $q - 1$ roots in C and so it determines a nonzero function on C. Suppose now that our claim is proved for $C[x_1, \dots, x_{n-1}]$ and $0 \neq g \in C[x_1, \dots, x_n]$ is a reduced polynomial. We write $g = \sum_{i=0}^{k} h_i(x_1, \dots, x_{n-1})x_n^i$ where $k < q$, $h_i \in C[x_1, \dots, x_{n-1}]$, $i = 0, 1, \dots, k$ and $h_k \neq 0$. Clearly all h_i are reduced polynomials. Since $h_k \neq 0$, by the induction assumption there exist elements $c_1, \dots, c_{n-1} \in C$ such that $h_k(c_1, \dots, c_{n-1}) \neq 0$. Then

$$p(x_n) = g(c_1, \dots, c_{n-1}, x_n) = \sum_{i=0}^{k} h_i(c_1, \dots, c_{n-1})x_n^i$$

is a nonzero reduced polynomial. Hence $p(c_n) \neq 0$ for some $c_n \in C$ and so $g(c_1, \dots, c_n) \neq 0$. The proof is thereby complete.

The $\mathcal{T}$-ideal of *GPI*'s on the ring of $n \times n$ matrices. In this subsection we determine $\mathcal{G}(R;\, R)$ for $R = M_n(C)$ (Proposition 6.5.5), and in the course of doing so we introduce the flavor of the arguments used in a more general situation.

Let C be a field, $n > 0$ a natural number and $A = M_n(C)$ the ring of $n \times n$-matrices over C. We fix a set $\mathcal{A} = \{e_{ij} \mid 1 \leq i, j \leq n\}$ of matrix units of A. Clearly $\mathcal{A}$ is a basis of the C-space A and it determines a monomial basis $\mathcal{M}(\mathcal{A})$ of $A_C{<}X{>}$ where $X = \{x_1, x_2, \dots, x_n, \dots\}$ is a countable set. We note that $\mathcal{M}(\mathcal{A})$ consists of all monomials of the form

$$M = e_{i_0j_1}x_{k_1}e_{i_1j_2}x_{k_2}\dots, x_{k_m}e_{i_mj_{m+1}}, \tag{6.9}$$

where $e_{i_{t-1}j_t} \in \mathcal{A}$, $x_{k_t} \in X$. Setting

$$\Lambda = \{[i, j],\ [i, k, j] \mid 1 \leq i, j \leq n,\ k \geq 1\},$$

we form the polynomial ring $C[\Lambda]$ over C. Define a linear mapping $\pi : A_C{<}X{>}\to C[\Lambda]$ by the rule

$$M^\pi = [i_0, j_{m+1}][j_1, k_1, i_1][j_2, k_2, i_2] \dots [j_m, k_m, i_m] \in C[\Lambda]$$

and its consequences where M is as in (6.9).

We fix any linear order of Λ such that $[i, j] < [r, k, s]$ for all $1 \le i, j, r, s \le n$, $k \ge 1$ and define a linear mapping $\eta : C[\Lambda] \to A_C{<}X{>}$ as follows. If a monomial $f \in C[\Lambda]$ is representable in the form

$$[i_0, j_{m+1}][j_1, k_1, i_1]^{n_1} \dots [j_m, k_m, i_m]^{n_m} \tag{6.10}$$

where $[j_t, k_t, i_t] < [j_{t+1}, k_{t+1}, i_{t+1}]$ for all $t = 1, 2, \dots, m-1$, then we set

$$f^\eta = e_{i_0 1}(e_{1j_1}x_{k_1}e_{i_1 1})^{n_1}(e_{1j_2}x_{k_2}e_{i_2 1})^{n_2} \dots (e_{1j_m}x_{k_m}e_{i_m 1})^{n_m} e_{1j_{m+1}}.$$

Otherwise we set $f^\eta = 0$.

Lemma 6.5.2 *Let*

$$M = e_{i_0 j_1} x_{k_1} e_{i_1 j_2} x_{k_2} \dots, x_{k_m} e_{i_m j_{m+1}} \in A_C{<}X{>} .$$

Then:

(i) *$M - M^{\pi\eta} \in \mathcal{T}(A;\ ST_2(e_{11};\ X))$=I;*

(ii) *If $|C| = q < \infty$, then*

$$M - M^{\pi\rho\eta} \in \mathcal{T}(A;\ ST_2(e_{11};\ X) + L_q(e_{11};\ X)) = J.$$

Proof. (i) Let $u(X), v(X) \in A_C{<}X{>}$. We claim that

$$e_{1j}ue_{k1}e_{1r}ve_{s1} - e_{1r}ve_{s1}e_{1j}ue_{k1} \in I$$

for all $1 \le j, k, r, s \le n$. Define an A-endomorphism

$$\phi : A_C{<}X{>}\to A_C{<}X{>}$$

by the rule

$$\begin{aligned} &\phi(x_1) = e_{1j}u(X)e_{k1},\ \phi(x_2) = e_{1r}v(X)e_{s1},\\ &\phi(x_t) = x_t \quad \text{for all} \quad t > 2. \end{aligned}$$

Then

$$e_{1j}ue_{k1}e_{1r}ve_{s1} - e_{1r}ve_{s1}e_{1j}ue_{k1} = \phi(ST_2(e_{11};\ X)) \in I.$$

and our claim is proved. The statement **(i)** follows now directly from the definitions of the mappings π and η.

(ii) Letting $L_q = L_q(e_{11}; X)$ and setting $x_2 = 0$, we infer that $L_q \in J$. Clearly

$$(e_{1j}u(X)e_{k1})^q - (e_{1j}u(X)e_{k1}) \in \mathcal{T}(A;\ L_q) \subseteq J$$

and so

$$M^{\pi\eta} - M^{\pi\rho\eta} \in \mathcal{T}(A;\ L_q) \subseteq J.$$

Now we have

$$M - M^{\pi\rho\eta} = M - M^{\pi\eta} + M^{\pi\eta} - M^{\pi\rho\eta} \in J$$

and the proof is thereby complete.

Corollary 6.5.3 *Let $h(X) \in A_C{<}X{>}$. Suppose that $h(X)^{\pi\eta} = 0$. Then $h(X) \in \mathcal{T}(A;\ ST_2(e_{11};\ X)) = I$.*

Proof. Writing $h(X) = \sum_M \alpha_M M$ where $M \in \mathcal{M}(\mathcal{A})$ and $0 \neq \alpha_M \in C$, we note that

$$h(X) = h(X) - h(X)^{\pi\eta} = \sum_M \alpha_M (M - M^{\pi\eta}) \in I$$

by Lemma 6.5.2. The proof is complete.

Analogously one can prove the following

Corollary 6.5.4 *Let $h(X) \in A_C{<}X{>}$. Suppose that $|C| = q < \infty$ and $h(X)^{\pi\rho\eta} = 0$. Then $h(X) \in \mathcal{T}(A;\, ST_2(e_{11};\, X) + L_q(e_{11};\, X))$.*

Proposition 6.5.5 *Let C be a field, $n > 0$ a natural number and $A = M_n(C)$ the ring of $n \times n$-matrices over the field C. Suppose that $h(x_1, x_2, \dots, x_r) \in A_C{<}X{>}$ is a GPI on A. Then:*

(i) If $|C| = \infty$ or $h(X)$ is multilinear, then

$$h(X) \in \mathcal{T}(A;\, ST_2(e_{11};\, X));$$

(ii) If $|C| = q < \infty$, then

$$h(X) \in \mathcal{T}(A;\, ST_2(e_{11};\, X) + L_q(e_{11};\, X)).$$

Proof. Clearly $h(X) = \sum_{i,j=1}^{n} e_{i1}(e_{1i}h(X)e_{j1})e_{1j}$ and all $e_{1i}h(X)e_{j1}$ are *GPI*s. Hence without loss of generality we can assume that $e_{11}h(X)e_{11} = h(X)$. Let $\gamma : C[\Lambda] \to C$ be any homomorphism of C-algebras such that $[1,1]^\gamma = 1$. We set

$$a_k = \sum_{j,i=1}^{n} e_{j,i}[j,k,i]^\gamma \quad \text{for all} \quad k = 1, 2, \dots.$$

Then for any monomial

$$M(x_1, x_2, \dots, x_r) = e_{1j_1}x_{k_1}e_{i_1j_2}x_{k_2}\dots x_{k_m}e_{i_m1}$$

we have

$$M(a_1, a_2, \dots, a_r) = e_{11}M^{\pi\gamma}.$$

Therefore

$$0 = h(a_1, a_2, \dots, a_r) = e_{11}h(X)^{\pi\gamma}$$

and $h(X)^{\pi\gamma} = 0$ for all $\gamma : C[\Lambda] \to C$. If $|C| = \infty$ or $h(X)$ is multilinear, then $h(X)^\pi = 0$. If $|C| = q < \infty$, then $h(X)^{\pi\rho} = 0$ by Remark 6.5.1. Applying Corollary 6.5.3 and Corollary 6.5.4, we complete the proof.

Lemma 6.5.6 *Let C be a field, $n > 0$ a natural number and $A = M_n(C)$ the ring of $n \times n$-matrices over the field C. Then:*

$$\mathcal{T}(A;\ St_{2n}(x_1, \ldots, x_{2n})) = \mathcal{T}(A;\ ST_2(e_{11};\ X)).$$

Proof. We have

$$St_{2n}(x_1, \ldots, x_{2n}) = \sum_{\sigma \in S_{2n}} \epsilon(\sigma) x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(2n)}$$

where S_{2n} is the symmetric group and $\epsilon(\sigma)$ is the sign of σ. Letting $h(x_1, \ldots, x_{2n})$ denote the polynomial in noncommutative indeterminates

$$\sum_{\substack{\sigma \in S_{2n} \\ \sigma(1) < \sigma(2)}} \epsilon(\sigma) x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(2n)},$$

we note that h is not a polynomial identity of A because

$$h(e_{11}, e_{11}, e_{12}, e_{22}, e_{23}, e_{33}, \ldots, e_{n-1,n} e_{nn}) = e_{1n} \neq 0.$$

Hence

$$p(x_1, x_2) = St_{2n}(x_1, x_2, e_{12}, e_{22}, e_{23}, \ldots, e_{n-1,n} e_{nn}) \neq 0.$$

By Amitsur-Levitsky theorem St_{2n} is a polynomial identity of A and so $p(x_1, x_2)$ is a GPI (see Theorem 1.3.5). Clearly

$$g(x_1, x_2) = e_{1i} p(x_1, x_2) e_{j1} \neq 0$$

for some $1 \leq i, j \leq n$. We write

$$g = \sum_{i,j,k,l=1}^{n} \beta_{ijkl} e_{1i} x_1 e_{jk} x_2 e_{l1} - \sum_{i,j,k,l=1}^{n} \delta_{ijkl} e_{1k} x_2 e_{li} x_1 e_{j1}$$

where $\beta_{ijkl}, \delta_{ijkl} \in C$ and pick $1 \leq i, j, k, l \leq n$ such that $\beta_{ijkl} \neq 0$. Then

$$\begin{aligned} f(x_1, x_2) &= g(e_{i1}x_1e_{1j}, e_{k1}x_2e_{1l}) \\ &= \beta_{ijkl}e_{11}x_1e_{11}x_2e_{11} - \delta_{ijkl}e_{11}x_2e_{11}x_1e_{11}. \end{aligned}$$

Clearly f is a GPI. In particular $f(e_{11}, e_{11}) = 0$ and so $\beta_{ijkl} = \delta_{ijkl}$. Therefore

$$ST_2(e_{11};\, X) = \beta_{ijkl}^{-1} f(x_1, x_2) \in \mathcal{T}(A;\, St_{2n}(x_1, \ldots, x_{2n}))$$

and hence

$$\mathcal{T}(A;\, St_{2n}(x_1, \ldots, x_{2n})) \supseteq \mathcal{T}(A;\, ST_2(e_{11};\, X)).$$

The converse inclusion follows from Proposition 6.5.5.

The $\mathcal{T}$-ideal of GPI's on primitive algebras over a field. In this rather lengthy subsection we determine $\mathcal{G}(R;\, R)$ for R a centrally closed prime ring over C. If R is not GPI then $\mathcal{G}(R;\, R) = 0$ and nothing more needs to be said. Therefore we may assume, in view of Theorem 6.1.6 and Theorem 4.3.7, that there exists an idempotent $w \in R$ such that $\Delta = wRw$ is a finite-dimensional division algebra over C whose center is wC.

We begin by looking at the case where $\Delta \cong C$, i.e. $wRw = Cw$. First of all we show that any $h \in R_C{<}X{>}$ has a so-called S-W-representation, which may then be used to develop a useful connection with a polynomial ring $C[\Lambda]$.

Let $h(x_1, x_2, \ldots, x_k) \in R_C{<}X{>}$. Clearly $h(X)$ is a sum of monomials of the form $a_1x_{k_1}a_2x_{k_2}\ldots a_mx_{k_m}a_{m+1}$ where $1 \leq k_i \leq k$, $a_j \in R$, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, m+1$. Letting V_h denote the C-subspace of R generated by all coefficients of $h(X)$ together with $\bar{1}$ and w, we note that $\dim_C(V_h) < \infty$. We note that V_h depends upon the choice of monomials in the representation of $h(X)$. By Litoff's theorem it follows that there exists an idempotent $u \in Soc(R)$ such that $uvu = v$ for all

$v \in V_h \cap Soc(R)$ and $uRu \cong M_t(C)$ for some natural number t. Since $w \in V_h \cap Soc(R)$, $uwu = w$ as well. Recalling that $wRw = wC$, we conclude that there exists a system of matrix units $W = \{e_{ij} \mid 1 \leq i,j \leq t\}$ such that $w = e_{11}$. Clearly $u = e_{11} + e_{22} + \ldots + e_{tt}$ and $V_h \cap Soc(R) \subseteq \sum_{ij} Ce_{ij}$. Choose elements $v_1 = \bar{1}, v_2, \ldots, v_m \in V_h$ such that they form a basis of V_h modulo $V_h \cap Soc(R)$. Obviously $V_h \subseteq \sum_{l=1}^{m} Cv_l + \sum_{i,j=1}^{t} Ce_{ij}$. Setting $S = \{v_1, v_2, \ldots, v_m\}$, we note that $h(X)$ is representable uniquely as a linear combination of monomials whose coefficients belongs to the set $S \cup W$. We will refer to this representation as an S-W-representation of $h(X)$. Let $h(X) = \sum \alpha_i h_i(X)$ be the S-W-representation of $h(X)$ where $0 \neq \alpha_i \in C$ and $h_i = h_j$ if and only if $i = j$. We consider monomials h_i as elements of the subsemigroup $\mathcal{S}$ of $R_C{<}X{>}$ generated by $S \cup W \cup X$. A submonomial (subword) g of h_i is said to be W-free if it belongs to the subsemigroup generated by $S \cup X$. Let H be the set of all W-free subwords of all monomials h_i. We consider the element $\bar{1}$ as a W-free submonomial of all monomials h_i. Clearly $|H| < \infty$. Setting

$$\Lambda = \{[g],\ [g;\ i],\ [j;\ g;\ i],\ [j;\ g] \mid g \in H,\ 1 \leq i,j \leq t\},$$

we form the polynomial ring $C[\Lambda]$ over C. We fix any linear order $<$ on Λ such that

$$[g;\ i] < [a;\ g';\ b] < [j;\ g'']$$

for all $g, g', g'' \in H$, $1 \leq i,j,a,b \leq t$. For any monomial h_s we have the following possibilities (the seemingly complicated description is simply a rigorous way of insuring that no element of S is ever adjacent to an e_{ij}):

(1) $h_s = g \in H$;

(2) $h_s = gx_re_{ij}$ for some $g \in H,\ 1 \leq r \leq k,\ 1 \leq i,j \leq t$;

(3) $h_s = e_{ij}x_rg$ for some $g \in H,\ 1 \leq r \leq k,\ 1 \leq i,j \leq t$;

(4) $h_s = gx_r e_{ij} x_l g'$ for some $g, g' \in H$, $1 \leq r, l \leq k$, $1 \leq i, j \leq t$;

(5) $h_s = g_0 e_{i_0 j_1} g_1 e_{i_1 j_2} \dots g_n e_{i_n j_{n+1}} g_{n+1}$
where :

(a) either $g_0 = \bar{1}$ or $g_0 = g_0' x_{r_0}$ for some $g_0' \in H$, $1 \leq r_0 \leq k$;

(b) either $g_i = x_{r_i}$ or $g_i = x_{r_i} g_i' x_{l_i}$ for some $g_i' \in H$, $1 \leq r_i, l_i \leq k$, where $1 \leq i \leq n$;

(c) either $g_{n+1} = \bar{1}$ or $g_{n+1} = x_{r_{n+1}} g_{n+1}'$ for some $g_{n+1}' \in H$, $1 \leq r_{n+1} \leq k$.

We define a polynomial $h_s^\pi \in C[\Lambda]$, respectively, in the cases just described:

Case 1 $h_s^\pi = [g]$;
Case 2 $h_s^\pi = [gx_r;\ i][j;\ \bar{1}]$;
Case 3 $h_s^\pi = [\bar{1};\ i][j;\ x_r g]$;
Case 4 $h_s^\pi = [gx_r;\ i][j;\ x_l g']$;
Case 5 $h_s^\pi = [g_0;\ i_0][j_1;\ g_1;\ i_1] \dots [j_n;\ g_n;\ i_n][j_{n+1};\ g_{n+1}]$.
Further we put

$$h^\pi = \sum \alpha_i h_i^\pi.$$

Consider a monomial $M \in C[\Lambda]$ which is written in the following form

$$P = [f_0;\ b_0][c_1;\ f_1;\ b_1] \dots [c_m;\ f_m;\ b_m][c_{m+1};\ f_{m+1}] \in C[\Lambda]$$

where $[c_i;\ f_i;\ b_i] \leq [c_{i+1};\ f_{i+1};\ b_{i+1}]$ for all $1 \leq i \leq m-1$. We set

$$\begin{aligned} P^\eta &= f_0 e_{b_0 c_1} f_1 e_{b_1 c_2} \dots f_m e_{b_m c_{m+1}} f_{m+1} \in R_C{<}X{>}, \\ ([g;\ i][j;\ \bar{1}])^\eta &= g e_{ij}, \\ ([\bar{1};\ i][j;\ g])^\eta &= e_{ij} g, \end{aligned}$$

$$\begin{aligned}([g;\, i][j;\, g'])^{\eta} &= g e_{ij} g',\\ [g]^{\eta} &= g.\end{aligned}$$

By linearity we extend η to linear combinations of the monomials just described. As in Lemma 6.5.2, Corollary 6.5.3 and Corollary 6.5.4 one can prove that

$$\begin{aligned}&h_s - h_s^{\pi\eta} \in \mathcal{T}(R;\, ST_2(w;\, X));\\ &\text{If}\quad |C| = q < \infty, \quad \text{then}\\ &h_s - h_s^{\pi\rho\eta} \in \mathcal{T}(R;\, ST_2(w;\, X) + L_q(w;\, X));\\ &\text{If}\quad h^{\pi\eta} = 0, \quad \text{then}\quad h(X) \in \mathcal{T}(R;\, ST_2(w;\, X));\\ &\text{If}\quad |C| = q < \infty \quad \text{and}\quad h^{\pi\rho\eta} = 0,\\ &\quad \text{then}\quad h \in \mathcal{T}(R;\, ST_2(w;\, X) + L_q(w;\, X)).\end{aligned}$$

We let $I = \mathcal{T}(R;\, ST_2(w; X))$ if h is multilinear or $|C| = \infty$, or $I = \mathcal{T}(R;\, ST_2(w; X) + L_q(w; X))$ if $|C| = q < \infty$. We therefore have the following sufficient condition for h to belong to I:

$$\begin{aligned}h^{\pi} &= 0 \quad (\text{if } h \text{ is multilinear or } |C| = \infty)\\ h^{\pi\rho} &= 0 \quad (\text{if } |C| = q < \infty)\end{aligned} \tag{6.11}$$

In view of Remark 6.5.1 (6.11) is equivalent to the single sufficient condition:

$$h^{\pi\gamma} = 0 \quad \text{for any } C\text{-algebra map } \gamma : C[\Lambda] \to C \tag{6.12}$$

We are now in a position to prove the key result of this subsection.

Theorem 6.5.7 *Let R be a primitive algebra with unity element $\bar{1}$ over a field C and let $\mathcal{G}(R;\, R) \subseteq R_C\langle X\rangle$ be the $\mathcal{T}$-ideal of GPI's on R. Assume that R contains a nonzero idempotent w such that $wRw = Cw$. Then:*

(i) If a GPI $h(X) \in R_C{<}X{>}$ is multilinear, then $h(X) \in \mathcal{T}(R;\ ST_2(w;\ X))$;

(ii) If $|C| = \infty$, then

$$\mathcal{G}(R;\ R) = \mathcal{T}(R;\ ST_2(w;\ X));$$

(iii) If $|C| = q < \infty$, then

$$\mathcal{G}(R;\ R) = \mathcal{T}(R;\ ST_2(w;\ X) + L_q(w;\ X)).$$

Proof. We shall assume that h is written in an S-W-representation and that linear maps π and η are as described near the beginning of this section. We shall prove all the statements of the theorem simultaneously. According to (6.12) it is suffices to show that $h^{\pi\gamma} = 0$ for all C-algebra maps $\gamma : C[\Lambda] \to C$. Unlike the simpler situation encountered in the proof of Proposition 6.5.5 the increased generality in the present situation entails a case-by-case series of technical arguments. We begin by setting the stage using Amitsur's Lemma.

We set

$$V = \sum_{s\in S}\sum_{j=1}^{t} Cse_{j1} \subseteq Re_{11}$$

and note that $V \supseteq \sum_{j=1}^{t} Ce_{j1}$ since $\bar{1} \in S$. By Lemma 4.2.8 there exist distinct elements $y_{g,i} \in Re_{11}$, $g \in H$, $0 \leq i \leq t$, such that the elements $\{sy_{g,i} \mid s \in S,\ g \in H,\ 0 \leq i \leq t\}$ are C-independent modulo the subspace V. In particular $sy_{g,i} = s'y_{g',i'}$ if and only if $(s; g; i) = (s'; g'; i')$.

Let $\gamma : C[\Lambda] \to C[\Lambda]$ be a homomorphism of C-algebras. We set

$$\begin{aligned} z_{g,0} &= y_{g,0} - uy_{g,0} + \sum_{j=1}^{t}[j;\ g]^{\gamma}e_{j1}, \\ z_{g,i} &= y_{g,i} - uy_{g,i} + \sum_{j=1}^{t}[j;\ g;\ i]^{\gamma}e_{j1} \end{aligned}$$

where $g \in H, 1 \leq i \leq t$. Let $s \in S$. Since $u = e_{11} + e_{22} + \ldots + e_{tt}$ and $suRe_{11} \subseteq \sum_{j=1}^{t} Cse_{j1} \subseteq V$, we have $sz_{g,i} \equiv sy_{g,i} \, (mod\, V)$ and so the elements

$$\{sz_{g,i} \mid s \in S,\ 0 \leq i \leq t\} \cup \{e_{j1} \mid 1 \leq j \leq t\}$$

are C-independent. Since $e_{11}Re_{11} = Ce_{11}$ and Re_{11} is a faithful irreducible left R-module, R is a dense subring of $End_C(Re_{11})$ by the Jacobson Density Theorem. Hence there exist elements

$$a, a_1, a_2, \ldots, a_k \in R$$

such that:

$$\begin{array}{ll}
\text{If} \quad x_r sg \in H, \quad \text{then} \quad a_r sz_{g,i} = z_{x_r sg,i}; & (6.13) \\
a_r e_{i1} = z_{x_r,i}; & (6.14) \\
\text{If} \quad sg \in H \quad \text{and} \quad i \geq 1, \quad \text{then} & \\
asz_{g,i} = [sg;\ i]^{\gamma} e_{11}; & (6.15) \\
\text{If} \quad sg \in H, \quad \text{then} \quad asz_{g,0} = [sg]^{\gamma} e_{11}; & (6.16) \\
ae_{i1} = [\bar{1};\ i]^{\gamma} e_{11}, & (6.17)
\end{array}$$

where $1 \leq r \leq k$, $s \in S$, $g \in H$, $1 \leq i \leq t$. Since $u = e_{11} + e_{22} + \ldots + e_{tt}$, $e_{1j}(y_{g,i} - uy_{g,i}) = 0$ and so

$$\begin{aligned}
e_{1j} z_{g,i} &= e_{1j} \left(y_{g,i} - uy_{g,i} + \sum_{j=1}^{t} [j;\ g;\ i]^{\gamma} e_{j1} \right) \\
&= [j;\ g;\ i]^{\gamma} e_{11} \qquad (6.18)
\end{aligned}$$

for all $1 \leq j \leq t$ and $g \in H$. Analogously

$$e_{1j} z_{g,0} = [j;\ g]^{\gamma} e_{11} \qquad (6.19)$$

for all $1 \leq j \leq t$ and $g \in H$. We claim that

$$ah_q(a_1, a_2, \ldots, a_k) z_{\bar{1},0} = h_q^{\pi\gamma} e_{11} \qquad (6.20)$$

for all monomials h_q involved in h. Indeed, consider the following five cases listed above.

Case 1. $h_q = g \in H$. Then it follows directly from (6.13) and (6.16) that

$$ah_q(a_1, a_2, \dots, a_k)z_{\bar{1},0} = [g]^\gamma e_{11} = [h_q]^\gamma e_{11}.$$

Case 2. $h_q = gx_r e_{ij}$. Then $e_{ij}z_{\bar{1},0} = [j; \bar{1}]^\gamma e_{i1}$ by (6.19). Further

$$a_r[j; \bar{1}]^\gamma e_{i1} = [j; \bar{1}]^\gamma z_{x_r,i}$$

by (6.14). Now from (6.13) and (6.15) we infer that

$$ah_q(a_1, a_2, \dots, a_k)z_{\bar{1},0} = [gx_r; i]^\gamma [j; \bar{1}]^\gamma e_{11} = [h_q]^\gamma e_{11}.$$

Case 3. $h_q = e_{ij}x_r g$. Then from (6.13) we conclude that $a_r g(a_1, \dots, a_k)z_{\bar{1},0} = z_{x_r g,0}$. Hence by (6.19) we have

$$e_{ij}a_r g(a_1, \dots, a_k)z_{\bar{1},0} = e_{ij}z_{x_r g,0} = [j; x_r g]^\gamma e_{i1}.$$

Applying (6.17) we obtain

$$ah_q(a_1, a_2, \dots, a_k)z_{\bar{1},0} = [j; x_r g]^\gamma [\bar{1}; i]^\gamma e_{11} = [h_q]^\gamma e_{11}.$$

Case 4. $h_q = gx_r e_{ij} x_l g'$. We already know that

$$e_{ij}a_l g'(a_1, \dots, a_k)z_{\bar{1},0} = [j; x_l g']^\gamma e_{i1}.$$

Applying (6.14) we obtain that

$$a_r e_{ij} a_l g'(a_1, \dots, a_k)z_{\bar{1},0} = [j; x_l g']^\gamma z_{x_r,i}.$$

Now from (6.13) and (6.15) we infer that

$$ah_q(a_1, a_2, \dots, a_k)z_{\bar{1},0} = [j; x_l g']^\gamma [i; gx_r]^\gamma e_{11} = [h_q]^\gamma e_{11}.$$

Case 5. $h_q = g_0 e_{i_0 j_1} g_1 e_{i_1 j_2} \dots g_n e_{i_n j_{n+1}} g_{n+1}$. We set

$$f = e_{i_0 j_1} g_1 e_{i_1 j_2} \dots g_n e_{i_n j_{n+1}} g_{n+1}$$

and note that $h_q = g_0 f$. If $g_{n+1} = \bar{1}$, then

$$e_{i_n j_{n+1}} z_{\bar{1},0} = [j_{n+1}; \bar{1}]^\gamma e_{i_n 1} = [j_{n+1}; g_{n+1}]^\gamma e_{i_n 1}.$$

If $g_{n+1} = x_{r_{n+1}} g'_{n+1}$, then we already know from *Case 3* that

$$\begin{aligned} e_{i_n, j_{n+1}} a_{r_{n+1}} g'_{n+1}(a_1, \ldots, a_k) z_{\bar{1},0} &= [j_{n+1}; x_{r_{n+1}} g'_{n+1}]^\gamma e_{i_n 1} \\ &= [j_{n+1}; g_{n+1}]^\gamma e_{i_n 1}. \end{aligned}$$

If $g_n = x_{r_n}$, then by (6.14) we have

$$a_{r_n} [j_{n+1}; g_{n+1}]^\gamma e_{i_n 1} = [j_{n+1}; g_{n+1}]^\gamma z_{x_{r_n}, i_n} = [j_{n+1}; g_{n+1}]^\gamma z_{g_n, i_n}.$$

If $g_n = x_{r_n} g'_n x_{l_n}$, then we infer from (6.14) and (6.13) that

$$a_{r_n} g'_n(a_1, \ldots, a_k) a_{l_n} [j_{n+1}; g_{n+1}]^\gamma e_{i_n 1} = [j_{n+1}; g_{n+1}]^\gamma z_{g_n, i_n}.$$

Therefore

$$\begin{aligned} & e_{i_{n-1} j_n} g_n(a_1, \ldots, a_k) e_{i_n j_{n+1}} g_{n+1}(a_1, \ldots, a_k) \\ &= [j_{n+1}; g_{n+1}]^\gamma e_{i_{n-1} j_n} z_{g_n, i_n} \\ &= [j_{n+1}; g_{n+1}]^\gamma [j_n; g_n; i_n]^\gamma e_{i_{n-1},1} \end{aligned}$$

by (6.18). Repeated application of the above argument yields that

$$f(a_1, a_2, \ldots, a_k) z_{\bar{1},0} = f^{\pi\gamma} e_{i_0,1}$$

and so

$$\begin{aligned} a h_q(a_1, \ldots, a_k) z_{\bar{1},0} &= a g_0(a_1, \ldots, a_k) f(a_1, \ldots, a_k) z_{\bar{1},0} \\ &= a g_0(a_1, \ldots, a_k) f^{\pi\gamma} e_{i_0,1}. \end{aligned}$$

If $g_0 = \bar{1}$, then by (6.17) we have

$$a f^{\pi\gamma} e_{i_0,1} = [\bar{1}; i_0]^\gamma f^{\pi\gamma} e_{11} = [g_0; i_0]^\gamma f^{\pi\gamma} e_{11} = h_q^{\pi\gamma} e_{11}.$$

If $g_0 = g'_0 x_{r_0}$, then from (6.14), (6.13) and (6.15) we infer that

$$a g_0(a_1, \ldots, a_k) f^{\pi\gamma} e_{i_0,1} = [g_0; i_0]^\gamma f^{\pi\gamma} e_{11} = h_q^{\pi\gamma} e_{11}$$

and our claim is thereby established.

Now from (6.20) it follows that

$$0 = ah(a_1, \ldots, a_k)z_{\bar{1},0} = h^{\pi\gamma}e_{11}$$

and so $h^{\pi\gamma} = 0$ for all C-algebra maps $\gamma : C[\Lambda] \to C$. The proof is thereby complete.

If h is a GPI on R, then the proof of the preceding theorem shows that condition (6.11), or equivalently (6.12), is a necessary and sufficient condition for an element $h \in R_C{<}X{>}$ to belong to the $\mathcal{T}$-ideal I. We proceed to draw further conclusions. If a monomial h_i appearing in h has a form described in **(1)** - **(4)**, then $h_i^{\pi} \neq h_j^{\pi}$ for any other monomial h_j appearing in the S-W-representation of $h(X)$. From this we conclude that monomials of the form described in **(1)** - **(4)** do not appear in $h(X)$ and so any monomial appearing in the S-W-representation of $h(X)$ has at least two coefficients in W. If either $h(X)$ is multilinear or $|C| = \infty$, then any monomial appearing in the S-W-representation of $h(X)$ has at least three coefficients in W. Given a natural number $s > 1$ we let $h_{(s)}$ denote the sum of all $\alpha_i h_i$ such that h_i has exactly $s - 1$ coefficients in W. We note that $h_{(s)}^{\pi}$ is exactly the s-homogeneous component of the polynomial h^{π}. Clearly a polynomial is equal to zero if and only if all its homogeneous components are equal to zero. Furthermore if $|C| = q < \infty$ and $f \in C[\Lambda]$ with homogeneous components $f_{(s)}$, then $f^{\rho} = 0$ if and only if $\sum\{f_{(i)} \mid i \equiv r \, mod\,(q-1)\} = 0$ for all $r = 1, 2, \ldots, q-1$.

Although the notion of an S-W-representation is a crucial one (it provides the important connection with the polynomial ring $C[\Lambda]$), it is not so natural to expect a given GPI h to be presented in such a restrictive representation. Fortunately we are able to partially loosen this restriction. To be sure we must continue to prescribe a subset S of elements of R of infinite rank which together with $\bar{1}$ is C-independent modulo $Soc(R)$.

However it is less artificial to assume now that h is a GPI on R which is written in the form $h = \sum \alpha'_j h'_j$, $0 \neq \alpha'_j \in C$, where the coefficients of all the h'_j's are either of finite rank or belong to S. As we have seen earlier the C-span of all coefficients of finite rank lies inside the C-span of a set W of matrix units e_{ij}, with e_{11} equal to the prescribed idempotent w. Thus we may also write h in its S-W-representation $h = \sum \alpha_i h_i$. It is clear that $h_{(s)}$ is equal to the sum of all $\alpha'_j h'_j$ such that h'_j has exactly $s-1$ coefficients of finite rank. The following corollary then follows from our discussion in the preceding paragraph.

Corollary 6.5.8 *Let R be a primitive algebra with unity element $\bar{1}$ over a field C having a nonzero idempotent w such that $wRw = Cw$ and let $h(X) = \sum \beta_i f_i$ be a GPI on R where $0 \neq \beta_i \in C$ and f_i's are monomials. Suppose that the set S of all coefficients of all f_i's of infinite rank together with $\bar{1}$ is C-independent modulo $Soc(R)$. Given a natural number $s \geq 1$ we set*

$$h_{(s)} = \sum \{\beta_i f_i \mid f_i \text{ has exactly } s-1 \text{ coefficients of finite rank}\}.$$

Then:

(i) $h_{(1)} = 0 = h_{(2)}$;

(ii) If either $h(X)$ is multilinear or $|C| = \infty$, then $h_{(3)} = 0$ and $h_{(k)}$ is a GPI on R for all $k > 3$;

(iii) If $|C| = q < \infty$, then

$$\sum_{s \equiv r \, mod \, (q-1)} h_{(s)}$$

is a GPI on R for all $r = 1, 2, \ldots, q-1$.

Let $h(X) = \sum \beta_i f_i$ be a GPI on R as in Corollary 6.5.8. Our aim now is to produce a closely related but simpler GPI $\sum \beta_i f'_i$ (see (6.21) ahead). Clearly any monomial f_i can be written in the following form:

$$f_i = g_{i0} y_{i0} a_{i0} y_{i1} g_{i1} x_{i1} a_{i1} \cdots y_{in_i} g_{in_i} x_{in_i} a_{in_i} y_{i,n_i+1} g_{i,n_i+1}$$

where the following conditions are fulfilled:

(i) $a_{ij} \in Soc(R)$, $j = 0, 1, \ldots, n_i$;

(ii) $x_{ij} \in X$, $y_{il} \in X \cup \{\bar{1}\}$, $1 \leq j \leq n_i$, $0 \leq l \leq n_i + 1$;

(iii) The g_{il} are alternating monomials in S and X such that if $y_{il} = \bar{1}$, then $g_{il} = \bar{1}$, $l = 0, 1, \ldots, n_i + 1$;

(iv) The set S of all (distinct) coefficients of all g_{ij} together with $\bar{1}$ is C-independent modulo $Soc(R)$.

Picking a C-basis of R modulo $Soc(R)$ containing $\bar{1}$ and all the coefficients of all the g_{ij}'s and extending it to a C-basis $\mathcal{A}$ of R, we note that $g_{ij} \in \mathcal{M}(\mathcal{A})$. We shall refer to the form of writing of h just described as an *$\mathcal{A}$-standard form* of writing of $h(X)$. Here we also note that any C-basis $\mathcal{A}'$ of R will be called *standard* if $\bar{1} \in \mathcal{A}'$ and $\mathcal{A}' \setminus Soc(R)$ is a C-basis of R modulo $Soc(R)$. Clearly the basis $\mathcal{A}$ just constructed is standard.

We set

$$g'_{i0} = g_{i0}y_{i0}, \quad g'_{i,n_i+1} = y_{i,n_i+1}g_{i,n_i+1}, \quad g'_{ij} = y_{ij}g_{ij}x_{ij}$$

where $1 \leq j \leq n_i$. Pick elements $z_{ij} \in X \cup \bar{1}$ such that:

(a) $z_{i0} = \bar{1}$ if and only if $g'_{i0} = \bar{1}$;

(b) $z_{i,n_i+1} = \bar{1}$ if and only if $g'_{i,n_i+1} = \bar{1}$;

(c) $z_{ij} \in X$ if $1 \leq j \leq n_i$;

(d) $z_{ij} = z_{pq}$ if and only if $g'_{ij} = g'_{pq}$.

Now we set

$$\begin{aligned} f'_i &= z_{i0}a_{i0}z_{i1}a_{i1}\ldots z_{in_i}a_{in_i}z_{i,n_i+1}, \\ h' &= \sum \beta_i f'_i. \end{aligned} \tag{6.21}$$

As we have earlier noted, without loss of generality we can assume that $a_{ij} \in \sum_{e \in W} Ce$ for all i, j. Also we can assume that all $z_{ij} \in H$ (just adjoin them to H). We write $h = \sum \alpha_i h_i$ in its S-W-representation. Now we have $h' = \sum \alpha_i h'_i$ where the monomials h'_i are obtained from the monomials h_i according to the above described procedure. We consider the case when either $h(X)$ is multilinear or $|C| = \infty$, since the case $|C| = q < \infty$

is considered analogously. Our comment after Theorem 6.5.7 indicates that $h^{\pi} = 0$. This means that for any monomial h_j appearing in the S-W-representation

$$\sum\{\alpha_i h_i^{\pi} \mid h_i^{\pi} = h_j^{\pi}\} = 0.$$

Since $h_i^{\pi} = h_j^{\pi}$ if and only if $(h_i')^{\pi} = (h_j')^{\pi}$, we conclude that $h'^{\pi} = 0$ and so by (6.11) h' is a GPI on R. Thus we have proved the following

Corollary 6.5.9 *Let R be a primitive algebra with unity element $\bar{1}$ over a field C having a nonzero idempotent w such that $wRw = Cw$, let $\mathcal{A}$ be a standard basis of R and let $h(X) = \sum \beta_i f_i$ be a GPI on R written in an $\mathcal{A}$-standard form. Then $h'(X)$ is a GPI on R where $h'(X)$ is obtained from $h(X)$ according to the procedure described in (6.21)*

Corollary 6.5.9 was pointed out to the first author by Prof. C.-L. Chuang in 1994, but no ideas of proof were presented.

Corollary 6.5.10 *Let R be a primitive algebra with unity element $\bar{1}$ over a field C having a nonzero idempotent w such that $wRw = Cw$, let $\mathcal{A}$ be a standard basis of R and let $h(X) = \sum \beta_i f_i$ be a GPI on R written in an $\mathcal{A}$-standard form. Further let $g = g'x_k$ where $g' \in \mathcal{M}(\mathcal{A})$ is a monomial without coefficients of finite rank and $x_k \in X$. We set*

$$I(g) = \{i \mid f_i = g a_i \widehat{h}_i \quad \textit{for some} \quad a_i \in Soc(R),\ \widehat{h}_i \in \mathcal{M}(\mathcal{A})\}.$$

Then $\widehat{h} = \sum_{i \in I(g)} \beta_i a_i \widehat{h}_i$ is a GPI on R.

Proof. We note that $\widehat{h}^{\pi}$ is exactly the sum of all $\alpha_i h_i^{\pi}$ such that h_i^{π} involves the variable of the form $[g; i]$, $1 \leq i \leq t$. We consider the case when $|C| = \infty$, since the case $|C| < \infty$ is considered analogously. Since h is a GPI on R, $h^{\pi} = 0$. Hence $\widehat{h}^{\pi} = 0$ and so $\widehat{h}$ is a GPI on R.

The following corollary answers a very natural question.

Corollary 6.5.11 *Let R be a primitive algebra with unity element $\bar{1}$ over a field C having a nonzero idempotent w such that $wRw = Cw$, $f, h \in R_C{<}X{>}$ and let $x_k \in X$ be a variable which is not involved in f and h. Suppose that fx_kh is a GPI on R and* $\deg_x(f) + \deg_x(g) < |C|$ *for all $x \in X$. Then either f or h is a GPI on R.*

Proof. Assume that neither f nor h is a GPI on R. As in the discussion at the beginning of this subsection we choose S and W such that both f and h have an S-W-representation (i.e., all their coefficients belong $\sum_{s\in S} Cs+\sum_{v\in W} Cv$). Let $f = \sum \alpha_i f_i$ and $h = \sum \beta_j h_j$ be S-W-representations. Then

$$\begin{aligned} f_i &= f_{i0}y_{i0}e_{p_{i0}q_{i1}}y_{i1}f_{i1}x_{i1}e_{p_{i1}q_{i2}}\cdots \\ &\quad y_{in_i}f_{in_i}x_{in_i}e_{p_{in_i}q_{i,n_i+1}}y_{i,n_i+1}f_{i,n_i+1} \end{aligned}$$

and

$$\begin{aligned} h_j &= h_{j0}z_{j0}e_{u_{j0}v_{j1}}z_{j1}h_{j1}t_{j1}e_{u_{j1}v_{j2}}\cdots \\ &\quad z_{jm_j}h_{jm_j}t_{jm_j}e_{u_{jm_j}v_{j,m_j+1}}z_{j,m_j+1}h_{j,m_j+1} \end{aligned}$$

where $x_{ij}, t_{rs} \in X$, $y_{ab}, z_{cd} \in X \cup \{\bar{1}\}$ satisfy the conditions **(iii)** and **(iv)** listed after Corollary 6.5.8.

We fix any $r = q_{i,n_i+1}$, $f' = y_{i,n_i+1}f_{i,n_i+1}$, $s = u_{j0}$ and $h' = h_{j0}z_{j0}$. Let $f_{(r,f')} = \hat{f}$ denote the sum of all $\alpha_l f_l$ such that $q_{l,n_l+1} = r$ and $y_{l,n_l+1}f_{l,n_l+1} = f'$ and let $h_{(s,h')} = \hat{h}$ denote the sum of all $\beta_l h_l$ such that $u_{l0} = s$ and $h_{l0}z_{l0} = h'$. Clearly $f = \sum f_{(r,f')}$ and $h = \sum h_{(s,h')}$. Since f and h are not GPI on R, we can choose r, f', s and h' such that $\hat{f}$ and $\hat{h}$ are not GPI on R.

We note that $(\hat{f}x_k\hat{h})^\pi$ is exactly the sum of all monomials (together with their coefficients) appearing in $(fx_kh)^\pi$ which involve the variable $[r; f'x_kh'; s]$. Recall that $\deg_x(f)+\deg_x(g) < |C|$. Hence if $|C| < \infty$, $(fx_kh)^{\pi\rho} = (fx_kh)^\pi$. Since fx_kh is a GPI on R, we infer from the proof of Theorem 6.5.7 that $(fx_kh)^\pi = 0$. It follows that $(\widehat{f}x_k\widehat{h})^\pi = 0$. But

$$(\widehat{f}x_k\widehat{h})^\pi = (\widehat{f})^\pi[r; f']^{-1}[r; f'x_kh'; s](\widehat{h})^\pi[h'; s]^{-1}.$$

Hence either $(\widehat{f})^\pi = 0$ or $(\widehat{h})^\pi = 0$ and respectively either $\widehat{f}$ is a GPI or $\widehat{h}$ is a GPI, a contradiction to the choice of $\widehat{f}$ and $\widehat{h}$. The proof is thereby complete.

Keep the notation of preceding corollary. Then setting $f = w$ and $h = x_1wx_kx_2w - x_2wx_kx_1w$ we see that

$$fx_kh = ST_2(w; x_kx_1, x_kx_2)$$

is a GPI on R. Therefore the condition that x_k is not involved in f and h is essential. Further let $|C| = q < \infty$. Setting $f = (wx_1w)^{q-1} + (wx_1w)^{q-2} + \ldots + w$ and $h = wx_1w - w$ we conclude that

$$fx_kh = wx_kwfh = wx_kwL_q(w; X)$$

is a GPI on R. Thus the condition $\deg_x(f) + \deg_x(h) < |C|$ for all $x \in X$ is essential as well.

We now come to the general situation in which R is a centrally closed prime GPI ring, i.e. there is a minimal idempotent w such that $\Delta = wRw$ is finite-dimensional over C. If C is finite, then $\Delta = C$ (by Theorem 4.2.3) in which case $\mathcal{G}(R; R)$ is already characterised in Theorem 6.5.7. Therefore without loss of generality we may assume for the remainder of this subsection that C is finite.

Let $n > 1$ be a natural number and $w \in R$. We set

$$ST_{2n}(w; X) = St_{2n}(wx_1, wx_2, \ldots, wx_{2n})w$$

where St_{2n} is the standard polynomial in $2n$ noncommuting variables.

Theorem 6.5.12 *Let R be a primitive algebra with identity over an infinite field C and let $\mathcal{G}(R;\, R)$ be the $\mathcal{T}$-ideal of GPI's on R. Assume that R has a nonzero idempotent w such that wRw is a division C-algebra of dimension n^2 over the field C and $Z(wRw) = wC$. Then:*

$$\mathcal{G}(R;\, R) = \mathcal{T}(R;\, ST_{2n}(w;\, X)).$$

Proof. One can easily show that R is a centrally closed prime ring with extended centroid C. Let C' be a maximal subfield of the division ring wRw. Clearly C' is a subalgebra of the C-algebra R. By Corollary 4.2.2 $wRw \otimes_C C' \cong M_n(C')$. Since $R' = R \otimes_C C' \supseteq wRw \otimes_C C'$, we conclude that R' has a nonzero idempotent w' such that $w'R'w' = w'C'$. From Theorem 2.3.5 it follows that R' is a closed prime C'-algebra. Hence the conditions of Theorem 6.5.7 hold in R' and

$$\mathcal{G}(R';\, R') = \mathcal{T}(R'; ST_2(w';\, X)). \tag{6.22}$$

Making use of the universal property of free algebras one can easily prove that $C{<}X{>} \otimes_C C' \cong C'{<}X{>}$ canonically. We will identify them. According to Remark 1.4.12 the C'-algebras $R_C{<}X{>} \otimes_C C'$ and $R'_{C'}{<}X{>}$ are isomorphic canonically. We will identify them. Further we will identify R with the subring $R \otimes 1$ of R'. Clearly

$$\mathcal{G}(R;\, R) \otimes_C C' \supseteq \mathcal{T}(R;\, ST_{2n}(w;\, X)) \otimes_C C'$$

are both ideals of $R'_{C'}{<}X{>}$. It is enough to show that

$$\mathcal{G}(R;\, R) \otimes_C C' \subseteq \mathcal{T}(R;\, ST_{2n}(w;\, X)) \otimes_C C'$$

To this end we claim that any GPI $h(X)$ on R is a GPI on R'. Indeed, since C is infinite, all homogeneous components of h are GPI's on R. Hence without loss of generality we can assume that $h(X)$ is homogeneous. Making use of induction on $ht(h)$, one can easily reduce consideration to the case when $h(X)$ is additive. But then it is immediate that $h(X)$ is a GPI on R'. Therefore

$$\mathcal{G}(R;\, R) \otimes_C C' \subseteq \mathcal{G}(R';\, R').$$

Next we claim that

$$\mathcal{T}(R;\, ST_{2n}(w;\, X)) \otimes_C C' = \mathcal{T}(R';\, ST_{2n}(w;\, X)).$$

Indeed, any R-endomorphism ϕ of $R_C{<}X{>}$ (i.e., any endomorphism such that $r^\phi = r$ for all $r \in R$) has a unique extension to an R'-endomorphism of $R'_{C'}{<}X{>}$ and so

$$\mathcal{T}(R;\, ST_{2n}(w;\, X)) \otimes_C C' \subseteq \mathcal{T}(R';\, ST_{2n}(w;\, X)).$$

On the other hand let ψ be an R'-endomorphism of $R'_{C'}{<}X{>}$. Pick any C-basis $v_1, v_2, \ldots, v_n$ of C' and write

$$x_i^\psi = \sum_{j=1}^{n} f_{ij} \otimes v_j,\ \ 1 \le i \le 2n.$$

Since $ST_{2n}(w;\, X)$ is multilinear, we have

$$(ST_{2n}(w;\, X))^\psi = \sum_{j_1 \ldots j_{2n}} v_{j_1} v_{j_2} \ldots v_{j_{2n}} ST_{2n}(w;\, f_{1j_1}, f_{2j_2} \ldots f_{2n,j_{2n}}).$$

As

$$ST_{2n}(w;\, f_{1j_1}, f_{2j_2} \ldots f_{2n,j_{2n}}) \in \mathcal{T}(R;\, ST_{2n}(w;\, X)),$$

we conclude that

$$(ST_{2n}(w;\, X))^\psi \subseteq \mathcal{T}(R;\, ST_{2n}(w;\, X)) \otimes_C C'$$

and so

$$\mathcal{T}(R;\, ST_{2n}(w;\, X)) \otimes_C C' \supseteq \mathcal{T}(R';\, ST_{2n}(w;\, X))$$

which proves our claim.

Secondly we note that

$$\begin{aligned}\mathcal{T}(R';\, ST_{2n}(w;\, X)) &\supseteq \mathcal{T}(wR'w;\, ST_{2n}(w;\, X)) \\ &= \mathcal{T}(wR'w;\, St_{2n}(X)).\end{aligned}$$

From Lemma 6.5.6 it now follows that

$$ST_2(w';X) \in \mathcal{T}(R';\, ST_{2n}(w;\, X))$$

and so

$$\mathcal{G}(R';\, R') \subseteq \mathcal{T}(R';\, ST_{2n}(w;\, X))$$

by Theorem 6.5.7. Summarizing what is proved, we see that

$$\begin{aligned}\mathcal{G}(R;\, R) \otimes_C C' &\subseteq \mathcal{G}(R';\, R') \\ &\subseteq \mathcal{T}(R';\, ST_{2n}(w;\, X)) \\ &= \mathcal{T}(R;\, ST_{2n}(w;\, X)) \otimes_C C' \\ &\subseteq \mathcal{G}(R;\, R) \otimes_C C'\end{aligned}$$

and hence

$$\mathcal{G}(R;\, R) \otimes_C C' = \mathcal{T}(R;\, ST_{2n}(w;\, X)) \otimes_C C'$$

which completes the proof.

Keep the notation of Theorem 6.5.12 and recall that we identified R and $R \otimes 1 \subseteq R \otimes_C C' = R'$. As an easy exercise we leave it to the reader to show that $Soc(R) \otimes_C C' = Soc(R')$. Clearly any C-basis $\mathcal{A}$ of R is a C'-basis of R'. Further, if $\mathcal{A}$ is a standard C-basis of R, then it is a standard C'-basis of R' as well. We are thus able to infer from Corollary 6.5.8, Corollary 6.5.9, Corollary 6.5.10, and Corollary 6.5.11 their respective analogues in the more general case where wRw is finite-dimensional over C. We shall merely state these, leaving the details of the proofs to the reader.

Corollary 6.5.13 *Let R be a primitive algebra with identity over an infinite field C having a nonzero idempotent w such that wRw is a finite dimensional division C-algebra with the center wC. Further let $\mathcal{A}$ be a standard C-basis of R and $h(X) = \sum \beta_i f_i$ a GPI on R written in an $\mathcal{A}$-standard form. Given a natural number $s \geq 1$ we set*

$$h_{(s)} = \sum \{\beta_i f_i \mid f_i \text{ has exactly } s-1 \text{ coefficients of finite rank}\}.$$

Then $h_{(1)} = h_{(2)} = h_{(3)} = 0$ and $h_{(k)}$ is a GPI on R for all $k > 3$.

Corollary 6.5.14 *Let R be a primitive algebra with identity over an infinite field C having a nonzero idempotent w such that wRw is a finite dimensional division C-algebra with the center wC. Further let $\mathcal{A}$ be a standard C-basis of R and $h(X) = \sum \beta_i f_i$ be a GPI on R written in an $\mathcal{A}$-standard form. Then $h'(X)$ is a GPI on R where $h'(X)$ is obtained from $h(X)$ according to the procedure described in (6.21)*

Corollary 6.5.15 *Let R be a primitive algebra with identity over an infinite field C having a nonzero idempotent w such that wRw is a finite dimensional division C-algebra with center wC. Further let $\mathcal{A}$ be a standard basis of R and let $h(X) = \sum \beta_i f_i$ be a GPI on R written in an $\mathcal{A}$-standard form. Let $g = g'x_k$ where $g' \in \mathcal{M}(\mathcal{A})$ be a monomial without coefficients of finite rank and $x_k \in X$. We set*

$$I(g) = \{i \mid f_i = g a_i \widehat{h}_i \quad \text{for some} \quad a_i \in Soc(R),\ \widehat{h}_i \in \mathcal{M}(\mathcal{A})\}.$$

Then $\widehat{h} = \sum_{i \in I(g)} \beta_i a_i \widehat{h}_i$ is a GPI on R.

Corollary 6.5.16 *Let R be a primitive algebra with identity over an infinite field C having a nonzero idempotent w such that wRw is a finite dimensional division C-algebra with center wC. Further let $f, h \in R_C{<}X{>}$ and let $x_k \in X$ be a variable which is not involved in f and h. Suppose that $f x_k h$ is a GPI on R. Then either f or h is a GPI on R.*

The $\mathcal{T}$-ideal of GPI's on semiprime rings. Throughout this subsection R will be a semiprime ring with extended centroid C, $Q = Q_{mr}(R)$, A the orthogonal completion of RC and $A \subseteq H \subseteq Q$ a C-algebra. We start with the following useful

Lemma 6.5.17 *Let R be a semiprime ring with extended centroid C and $B = B(C)$. Then there exists an orthogonal subset $\{e_i \mid i = 2, 3, \ldots\} \subseteq B$ such that:*

(i) For any $M \in Spec(B)$ $|\phi_M(C)| = n > 1$ if and only if $e_n \notin M$;

(ii) $x^n = x$ for all $x \in e_nC$.

Proof. First of all we recall that $\phi_M(C)$ is a field. Consider the sentences

$$\begin{aligned}\Psi_n &= (\exists x_1)\ldots(\exists x_n)(\forall y)(\wedge_{i\neq j}||x_i \neq x_j||) \wedge ||y \in C|| \\ &\quad \wedge(\wedge_{i=1}^n ||x_i \in C||) \wedge (||\prod_{i=1}^n (y - x_i) = 0||)\end{aligned}$$

where $n = 2, 3, \ldots$. Clearly the Ψ_n's are Horn formulas. Setting $e_n = E(\Psi_n) \in B$, $n = 2, 3, \ldots$, we infer from Theorem 3.2.10 that $|\phi_M(C)| = n$ if and only if $e_n \notin M$.

Now we consider the sentences

$$\Phi_n = (\forall x)||x \in C|| \wedge ||x^n = x||, \quad n = 2, 3, \ldots.$$

Note that the Φ_n's are Horn formulas. If $|\phi_M(C)| = n$, then we have $\phi_M(C) \models \Phi_n$. Therefore $e_n \notin M$ implies that $E(\Phi_n) \notin M$ and so $E(\Phi_n)e_n = e_n$ (see Theorem 3.2.10). From the definition of the idempotents $E(\Phi_n)$ we infer that $e_nC \models \Phi_n$ which means that $x^n = x$ for all $x \in e_nC$. The proof is complete.

We remark that in Lemma 6.5.17 some or all of the e_i's may be 0.

Lemma 6.5.18 *Let R be a semiprime ring with extended centroid C, $Q = Q_{mr}(R)$ and A the orthogonal completion of the* *central closure $RC \subseteq Q$ of R. Further let idempotents $e_2, e_3, \ldots$ be as in Lemma 6.5.17. Suppose that R has a strict generalized polynomial identity $h(X) \in Q_C{<}X{>}$. Then there exist idempotents $v_2, v_3, \ldots \in A$ such that $E(v_i) = e_i$ and $v_iQv_i = v_iC$ for all $i = 2, 3, \ldots$. Furthermore $L_n(v_n; X) = (v_nx_1v_n)^n - v_nx_1v_n$ is a GPI on Q for all $n = 2, 3, \ldots$.*

Proof. We first note that if $e_i = 0$ then one need only choose $v_i = 0$. Thus we shall only be concerned with those e_i for which $e_i \neq 0$. Consider the sentence

$$\begin{aligned}\Psi \quad = \quad & (\exists x)(\forall y)(\exists z)(\forall t)\|x^2 = x\| \wedge \|z \in C\| \\ & \wedge\|t \in C\| \wedge \|xyx = xz\| \wedge (\|tx \neq 0\| \vee \|t = 0\|).\end{aligned}$$

Clearly Ψ is a Horn formula. Let $B = B(C)$ and $M \in Spec(B)$. Suppose that $e_n \notin M$. As we already know then $|\phi_M(C)| = n$. By Corollary 6.3.10 $\phi_M(A)$ is a primitive ring with nonzero idempotent w such that $w\phi_M(A)w$ is division ring finite dimensional over $\phi_M(C)$. From Wedderburn's Theorem we infer that $w\phi_M(A)w$ is commutative and hence is equal to $w\phi_M(C)$ (see Theorem 4.2.3). Therefore $\phi_M(A) \models \Psi$, whence $E(\Psi) \notin M$ by Theorem 3.2.10. We conclude that $E(\Psi)e_n = e_n$ and $e_nA \models \Psi$, which means that e_nA contains an idempotent v_n such that $v_n(e_nA)v_n = v_n(e_nC)$ and $r_{e_nC}(v_n) = 0$. Hence $E(v_n) = e_n$, $e_nv_n = v_n$ and $v_nAv_n = v_nC$. Since $v_nC \cong e_nC$, it follows from Lemma 6.5.17 that $L_n(v_n; X)$ is a GPI on A. Applying Theorem 6.4.1, we complete the proof.

Now we are in a position leading up to the main results of the present section, namely, to give a list of generators for the $\mathcal{T}$-ideal $\mathcal{G}(H; R)$ and a criterion for this $\mathcal{T}$-ideal to be finitely generated. We make the natural assumption that R has a strict GPI $h(X) \in Q_C{<}X{>}$. Let $u_1, u_2, \ldots, u_t$ be the idempotents given by Theorem 6.3.9, recalling that each u_i is an $E(u_i)C$-faithful abelian idempotent of $E(u_i)C$-rank $n_i = k_i^2$. We claim that each $S_i = ST_{2k_i}(u_i;\, X)$ is a *GPI* on Q. Indeed, let

$$\Psi_i = (\forall r_1)(\forall r_2)\dots(\forall r_{2k_i})\|ST_{2k_i}(r_1, r_2, \dots, r_{2k_i}) = 0\|.$$

Let $M \in Spec(B)$. If $\phi_M(u_i) = 0$, then $ST_{2k_i}(\phi_M(u_i); X) = 0$ and so $\phi_M(Q) \models \Psi_i$. Suppose now that $\phi_M(u_i) \neq 0$. Then by Theorem 6.3.9 $\phi_M(u_iQu_i)$ is n_i-dimensional division algebra over its center $\phi_M(u_iC)$. According to Corollary 4.2.2 the ring $\phi_M(u_iQu_i)$ is embeddable into $k_i \times k_i$ matrix ring over a field. Then by Theorem 1.3.5 we see that $St_{2k_i}(X)$ is a polynomial identity of $\phi_M(u_iQu_i)$. It follows that $\phi_M(Q) \models \Psi_i$ for all $M \in Spec(B)$. By Theorem 3.2.10 we have that $E(\Psi_i) \notin M$ for all $M \in Spec(B)$. Therefore $E(\Psi_i) = 1$, $ST_{2k_i}(u_i;\, X)$ is a *GPI* on Q and our claim is established. Further let $v_{i_1}, v_{i_2}, \dots, v_{i_k}, \dots$ (possibly empty or infinite in number) be the nonzero idempotents given in Lemma 6.5.18, and so we know that each $L_{i_j} = L_{i_j}(v_{i_j};\, X)$ is also a *GPI* on Q. We set

$$\mathcal{P} = \{S_1, S_2, \dots, S_t, L_{i_1}, L_{i_2}, \dots, L_{i_k}, \dots\}$$

and show in Theorem 6.5.19 that $\mathcal{P}$ is a set of generators of the $\mathcal{T}$-ideal $\mathcal{G}(H;\, R)$.

In preparation for this theorem we continue with the following remarks. It follows from Theorem 6.4.1 that $\mathcal{G}(H;\, R) = \mathcal{G}(H;\, H)$. Let $B = B(C)$. Since C is von Neumann regular, the mapping $Spec(C) \to Spec(B)$ given by the rule $P \mapsto P \cap B$, $P \in Spec(C)$, is a bijection with the inverse mapping given by the rule $M \mapsto CM$, $M \in Spec(B)$. For any $M \in Spec(B)$ let ϕ_M denotes the canonical homomorphism of rings $Q \to \overline{Q} = Q/MQ$. We set $\overline{A} = \phi_M(A)$, $\overline{C} = \phi_M(C)$ and $\overline{H} = \phi_M(H)$. As we already know $\overline{A}$ is a prime ring with the extended centroid $\overline{C}$ and $\overline{Q} \subseteq Q_{mr}(\overline{A})$ (see Theorem 3.2.7 and Theorem 3.2.15).

Letting Φ_M denote the canonical extension of ϕ_M to666 Q_C< X>$\to$ $\overline{Q}_{\overline{C}}$<$X$>, we infer from Remark 6.3.5 and Corollary 6.3.6 that Φ_M is surjective and $\Phi_M(h)$ is a nonzero *GPI* on $\overline{H}$. Since

$\overline{H}$ is centrally closed with the extended centroid $\overline{C}$, we conclude that it is a primitive ring with a nonzero idempotent w such that $w\overline{H}w$ is a finite dimensional $\overline{C}$-algebra with center $w\overline{C}$ (see Theorem 6.1.6). Therefore the $\overline{C}$-algebra $\overline{H}$ satisfies all the conditions either of Theorem 6.5.7 (if $w\overline{H}w$ is commutative) or of Theorem 6.5.12 (if $w\overline{H}w$ is not commutative).

We claim that

$$\Phi_M(\mathcal{G}(H;\ H)) = \mathcal{G}(\overline{H};\ \overline{H}).$$

Indeed, we already know that $\Phi_M(\mathcal{G}(H;\ H)) \subseteq \mathcal{G}(\overline{H};\ \overline{H})$. Suppose now that $\Phi_M(f)$ is a GPI on $\overline{H}$ where

$$f = f(x_1, x_2, \dots, x_n) \in Q_C{<}X{>} .$$

We consider the formula

$$\Psi = (\forall r_1)\dots(\forall r_n)\|f(r_1, r_2, \dots, r_n) = 0\|.$$

Let $a_1, a_2, \dots, a_m \in H$ be all the coefficients appearing in f. Considering them as 0-ary operations of the orthogonally complete Ω-Δ-ring Q where

$$\Omega = \{0, 1, a_1, a_2, \dots, a_n, -, +, \cdot\}$$

and $\Delta = \{\|x = y\|\}$, we note that Ψ is a Horn sentence. If $\overline{Q} \models \Psi$, then there exists an idempotent $e \in B \setminus M$ such that $eQ \models \Psi$ (see Theorem 3.2.10). This means that ef is a GPI on eQ and hence it is a GPI on Q. Therefore $ef \in \mathcal{G}(H;\ H)$. Since $\Phi_M(ef) = \Phi_M(f)$, we conclude that $\Phi_M(\mathcal{G}(H;\ H)) \supseteq \mathcal{G}(\overline{H};\ \overline{H})$ which proves our claim.

Now we consider any H-endomorphism τ of $H_C{<}X{>}$ (i.e., an endomorphism τ such that $a^\tau = a$ for all $a \in H$). Clearly it induces an $\overline{H}$-endomorphism $\overline{\tau}$ of $\overline{H}_{\overline{C}}{<}X{>}$. We claim that any $\overline{H}$-endomorphism σ of $\overline{H}_{\overline{C}}{<}X{>}$ is of this form. Indeed, pick $g_x \in H_C{<}X{>}$ such that $x^\sigma = \Phi_M(g_x)$ for all $x \in X$ and define the H-endomorphism τ of $H_C{<}X{>}$ by the rule $x^\tau = g_x$, $x \in X$, and its consequences. Obviously $\overline{\tau} = \sigma$ and our claim is proved. Now it follows that for any subset $F \subseteq H_C{<}X{>}$ we have

$$\Phi_M(\mathcal{T}(H;\, F)) = \mathcal{T}(\overline{H};\, \Phi_M(F)).$$

Theorem 6.5.19 *Let R be a semiprime ring with extended centroid C and $Q = Q_{mr}(R)$. Further let A be the orthogonal completion of the subalgebra $RC + C \subseteq Q$. Suppose that R has a strict GPI $h(X) \in Q_C < X >$ and $A \subseteq H \subseteq Q$ is a C-subalgebra. Then $\mathcal{P}$ (given above) is a set of generators for the $\mathcal{T}$-ideal $\mathcal{G}(H;\, R)$ of all generalized identities on R.*

Proof. In view of $\mathcal{G}(H;\, R) = \mathcal{G}(H;\, H)$ and the fact that $\mathcal{T}(H;\, \mathcal{P}) \subseteq \mathcal{G}(H;\, H)$ we need only show that

$$\mathcal{G}(H;\, H) \subseteq \mathcal{T}(H;\, \mathcal{P}).$$

For any $M \in Spec(B)$ we have $\mathcal{G}(\overline{H};\, \overline{H}) = \mathcal{T}(\overline{H};\, \Phi_M(\mathcal{P}))$ by Theorem 6.5.7 and Theorem 6.5.12, and hence

$$\Phi_M(\mathcal{G}(H;\, H)) = \mathcal{G}(\overline{H};\, \overline{H}) = \mathcal{T}(\overline{H};\, \Phi_M(\mathcal{P})) = \Phi_M(\mathcal{T}(H;\, \mathcal{P}))$$

by the remark preceding the statement of this theorem. Now consider any element $f \in \mathcal{G}(H;\, H)$. Then for each $M \in Spec(B)$ $\Phi_M(f) = \Phi_M(h_M)$ for some $h_M \in \mathcal{T}(H;\, \mathcal{P})$. By Remark 3.2.2(**i**) $v_M(f - h_M) = 0$ for some $v_M \in B \setminus M$. We note that $v_M f = v_M h_M$. By Lemma 3.1.21 (with suitable relabeling of subscripts) there is a finite subset $v_1, v_2, \ldots, v_s$ of the v_M's for which there are central idempotents $0 \neq e_i \leq v_i$, $e_1 + e_2 + \ldots + e_s = 1$, and $e_i e_j = 0$ for $i \neq j$. Therefore for each $j = 1, 2, \ldots, s$ $e_j f = e_j h_M = h_j \in \mathcal{T}(H;\, \mathcal{P})$ and so $f = \sum_{j=1}^{s} e_j f \in \mathcal{T}(H;\, \mathcal{P})$. The proof is complete.

As our final result in this section we have

Theorem 6.5.20 *Under the assumptions and notation of Theorem 6.5.19 the following conditions are equivalent:*

(i) $\mathcal{G}(H;\, R)$ *is finitely generated as a* $\mathcal{T}$*-ideal;*

(ii) There is a natural number N *such that for any maximal ideal* P *of* C *either* $|C/P| \le N$ *or* $|C/P| = \infty$.

Proof. **(i) ⇒ (ii)** Let F be a finite generating set of $\mathcal{G}(H;\, R) = \mathcal{G}(H;\, H)$ and $m = \max_{f\in F}\deg(f)$. Further let $M \in Spec(B)$ and $|\phi_M(C)| = n < \infty$. It is enough to show that $n \le m$. Suppose that $n > m$. Using Vandermonde determinant arguments, one can easily show that all homogeneous components of any $f \in \Phi_M(F)$ are a GPI's on $\overline{H}$. Letting F' denote the set of all homogeneous components of all $f \in \Phi_M(F)$, we note that

$$\begin{aligned}\mathcal{G}(\overline{H};\, \overline{H}) &= \Phi_M(\mathcal{G}(H;\, H)) = \Phi_M(\mathcal{T}(H;\, F))\\ &= \mathcal{T}(\overline{H};\, \Phi_M(F)) = \mathcal{T}(\overline{H};\, F').\end{aligned}$$

Further as we already know from the proof of Lemma 6.5.18, $\overline{H}$ contains a nonzero idempotent w such that $w\overline{H}w = w\overline{C}$ and $L_n(w;\, X)$ is a GPI on $\overline{H}$. Therefore

$$L_n(w;\, X) \in \mathcal{T}(\overline{H};\, F'). \tag{6.23}$$

Let K be the field of rational expressions in t with coefficients in $\overline{C}$. We identify the ring $\overline{H}$ with the subring $1\otimes\overline{H} \subseteq K\otimes_{\overline{C}}\overline{H} = G$. Clearly $wGw = wK$ and $G = \overline{H}K$. Using the induction on the height of GPI and the relations $\deg(f) < |C|$ for all $f \in F'$, one can prove that every $f \in F'$ vanishes on G (see the proof of Lemma 6.4.3 for the details). It follows from (6.23) that $L_n(w;\, X)$ vanishes on G which means that $(wk)^n = wk$ for all $k \in K$, a contradiction. Thus $n \le m$.

(ii) ⇒ (i) By Theorem 6.5.19

$$\mathcal{P} = \{S_1, S_2, \ldots, S_t, L_{i_1}, L_{i_2}, \ldots, L_{i_k}, \ldots\}$$

is a set of generators for the $\mathcal{T}$-ideal $\mathcal{G}(H;\, R)$. We claim that $i_k \le N$ for all k. Indeed, if $i_k > N$, we choose $M \in Spec(B)$ such that $E(v_{i_k}) \notin M$. Then by Lemma 6.5.18 and Lemma 6.5.17(**i**) we have that $|\phi_M(C)| = i_k > N$ forcing the contradiction to our assumptions. Therefore our claim is established. But then $\mathcal{P} = \{S_1, \ldots, S_t, L_{i_1}, \ldots, L_{i_s}\}$ for some s such that $i_s \leq N$ and so $\mathcal{G}(H;\, R)$ is finitely generated as a $\mathcal{T}$-ideal. The proof is complete.

Theorem 6.5.7, Theorem 6.5.12 and Theorem 6.5.19 were proved by K. I. Beidar (see [23] and [26]). The case of generalized polynomial identities with involution was considered in [250], [237], [238], and [239]. Corollary 6.5.9 was pointed out to him by Prof. C.-L. Chuang in 1994, but no ideas of proof were presented.

6.6 Special *GPI*'s

In this section we shall discuss some special generalized polynomial identities. We start with the following

Lemma 6.6.1 *Let V be a nonzero right vector space over a division ring Δ with proper subspaces $V_1, V_2, \ldots, V_n$ such that $V = \cup_{i=1}^n V_i$. Then Δ is a finite field with $|\Delta| < n$.*

Proof. Without loss of generality we may assume that $\cup_{i \neq j} V_i \neq V$ for all $j = 1, 2, \ldots, n$. Pick $v_j \in V \setminus \cup_{i \neq j} V_i$. We note that $v_j \in V_i$ if and only if $i = j$. Thus if $\lambda v_j \in V_i$, $0 \neq \lambda \in \Delta$, then $v_j \in V_i$ forcing $i = j$. The case $n = 2$ cannot exist and so we may assume $n > 2$. Suppose $|\Delta| \geq n$. Then (by the pigeon-hole principle) there exists $i > 2$ such that $v_1 + \lambda v_2, v_1 + \mu v_2 \in V_i$ for some $\lambda \neq \mu \in \Delta$. Thus $\lambda\mu^{-1}v_1 + \lambda v_2 \in V_i$ and so $(1 - \lambda\mu^{-1})v_1 \in V_i$, forcing the contradiction $\lambda = \mu$. By Theorem 4.2.3 Δ is a field and the proof is complete.

Theorem 6.6.2 *Let R be a prime ring with extended centroid C and $Q = Q_{mr}(R)$. Then the following conditions are equivalent:*

(i) *There exist nonzero elements $r_1, r_2, \ldots, r_{n+1} \in R$ such that $r_1 x r_2 x \ldots r_n x r_{n+1} = 0$ for all $x \in R$;*

(ii) *There exist nonzero elements $q_1, q_2, \ldots, q_{n+1} \in Q$ such that $q_1 x q_2 x \ldots q_n x q_{n+1} = 0$ for all $x \in R$;*

(iii) *$|C| \leq n$ and R is a noncommutative primitive ring with nonzero socle containing a minimal idempotent e such that $eRe = eC$.*

Proof. The implication **(i)** ⇒ **(ii)** is obvious. We show that **(ii)** ⇒ **(iii)**. Clearly

$$q_1 x q_2 x \ldots q_n x q_{n+1} \tag{6.24}$$

is a GPI on R. In view of Proposition 6.4.2 it is enough to show that $|C| \leq n$. By Theorem 6.4.4 $q_1 x q_2 x \ldots q_n x q_{n+1} = 0$ for all $x \in Q$ and so Q is GPI. In particular Q is a primitive ring with nonzero socle K. Let e be a minimal idempotent of Q. Consider the right vector space $V = Qe$ over the division ring $\Delta = eQe$. Clearly $Q \subseteq End(V_\Delta)$ and $\ker(q_i)$ is a subspace of V for all $i = 1, 2, \ldots, n+1$. If $V = \cup_{i=1}^{n+1} \ker(q_i)$, then by Lemma 6.6.1 $|\Delta| \leq n$ and so $|C| \leq n$. Hence without loss of generality we may assume that $\cup_{i=1}^{n+1} \ker(q_i) \neq V$ and there exists $q \in Q$ such that $q_i q e \neq 0$ for all $i = 1, 2, \ldots, n+1$. Substituting qex for x in (6.24) and multiplying by qe from the right, we infer that

$$q_1 qex q_2 qex \ldots q_n qex q_{n+1} qe \tag{6.25}$$

is a nonzero GPI on Q. Now we consider the faithful right Q-module $W = eQ$. If $W \neq \cup_{i=1}^{n+1} \ker q_i qe$, then there exists $q' \in Q$ such that $eq' q_i qe \neq 0$ for all $i = 1, 2, \ldots, n+1$. Since $\Delta = eQe$ is a division ring, we conclude that

$$\begin{aligned}&(eq')[(q_1 qe)(eq')(q_2 qe)(eq') \ldots (q_n qe)(eq')(q_{n+1} e)\\&= (eq' q_1 qe)(eq' q_2 qe) \ldots (eq' q_{n+1} qe) \neq 0,\end{aligned}$$

a contradiction to (6.25). Thus $W = \cup_{i=1}^{n+1} \ker q_i qe$ and so $|\Delta| \leq n$ by Lemma 6.6.1.

(iii) ⇒ (i) Clearly $Soc(R)$ contains an idempotent v such that $vRv \cong M_2(C)$. Let $\{e_{ij} \mid 1 \leq i,j \leq 2\}$ be matrix units of vRv. Obviously $vRv = End_C(vRe_{11})$ and the vector space vRe_{11} contains exactly $m = |C|+1 \leq n+1$ distinct one dimensional subspaces $V_1, V_2, \ldots, V_m$. It is well-known that any proper subspace of a vector space is the kernel of a nonzero linear endomorphism. Pick $a_i \in vRv$ such that $V_i = \ker(a_i)$, $i = 1, 2, \ldots, m$. Further choose $b_i \in vRv$ such that $r_i = e_{11}b_i a_i \neq 0$. We set $r_{m+1} = e_{11}$. Then for all $x \in R$ we have

$$\begin{aligned}&r_1 x r_2 x \ldots r_m x r_{m+1}\\ &= e_{11}b_1[a_1(vxe_{11})]b_2[a_2(vxe_{11})]\ldots[a_m(vxe_{11})] = 0\end{aligned}$$

since $vxe_{11} \in V_i$ for some $1 \leq i \leq m$. The proof is complete.

Corollary 6.6.3 *Let $n > 0$ be a natural number and R a prime ring with infinite extended centroid. Further let $r_1, r_2, \ldots, r_{n+1} \in R$. Suppose that $r_1 x r_2 x \ldots r_n x r_{n+1} = 0$ for all $x \in R$. Then $r_i = 0$ for some $1 \leq i \leq n+1$.*

Proof. Let C be the extended centroid of R. Then $|C| > n$. Now apply Theorem 6.6.2.

Proposition 6.6.4 *Let R be a semiprime ring with extended centroid C and $Q = Q_{mr}(R)$. Further let $B = B(C)$, $M \in Spec(B)$ and $\phi_M : Q \to Q/MQ$ the canonical surjection of rings. Suppose $\phi_M(Q)$ is GPI with $|\phi_M(C)| = m < \infty$. Then there exists an idempotent $e \in B \setminus M$ such that every right (left) ideal L of R with $eL \neq 0$ contains a nonzero idempotent $w \in L$ such that wRw is a commutative ring and $x^m = x$ for all $x \in wRw$.*

Proof. Let $H = Q_s(R)$. Consider the formula

$$\begin{aligned}\Phi \quad = \quad & (\exists v)(\forall c_1)(\forall x)(\exists c_2)\|c_1 \in C\| \wedge \|c_1^m = c_1\| \\ & \wedge(\|c_1 = 0\| \vee \|c_1 v \neq 0\|) \wedge \|c_2 \in C\| \\ & \wedge\|vxv = vc_2\| \wedge \|v^2 = v\| \end{aligned} \tag{6.26}$$

Clearly Φ is Horn sentence. It follows from Proposition 6.4.2 that $\phi_M(H) \models \Phi$. By Theorem 3.2.10 $e = E(\Phi) \notin M$ and $eH \models \Phi$. Hence there exists an idempotent $v \in H$ such that $E(v) = e$ and $vHv = vC$. We also note that $x^m = x$ for all $x \in eC$.

Now let L be a right ideal of R such that $eL \neq 0$. Then $ae \neq 0$ for some $a \in L$ and so $eE(a) \neq 0$. Pick any $N \in Spec(B)$ such that $E(a)e \notin N$. According to Corollary 3.2.4 $\overline{a} = \phi_N(a) \neq 0$ and $\overline{v} = \phi_N(v) \neq 0$. Clearly $\overline{v}\overline{H}\overline{v} = \overline{v}\overline{C}$ and $x^m = x$ for all $x \in \overline{C}$ where $\overline{H} = \phi_N(H)$ and $\overline{C} = \phi_N(C) = \phi_N(eC)$. Clearly $\overline{H}$ is a primitive ring with nonzero socle and $\overline{v}$ is a minimal idempotent of $\overline{H}$. By Theorem 4.3.7(**ii**) the right ideal $\overline{a}\overline{H}$ contains a minimal idempotent u. Obviously $u\overline{H}u = u\overline{C}$. Consider the formula (here we note that it is understood that the element a is a 0-ary operation on H)

$$\begin{aligned}\Psi \quad = \quad & (\exists b)(\forall c_1)(\forall x)(\exists c_2)\|c_1 \in C\| \wedge \|c_1^m = c_1\| \wedge \|(\overline{a}b)^2 = \overline{a}b\| \\ & \wedge(\|c_1 = 0\| \vee \|c_1\overline{a}b \neq 0\|) \wedge \|c_2 \in C\| \wedge \|\overline{a}bx\overline{a}b = \overline{a}bc_2\|. \end{aligned}$$

By the preceding observations $\overline{H} \models \Psi$. It follows from Theorem 3.2.10 that $fH \models \Psi$ for some $f \notin N$. Hence there exists an idempotent $w' \in aH$ such that $E(w') = f$ and $w'Hw' = w'C$. Furthermore $x^m = x$ for all $x \in fC$. Since $fC \cong w'C$, we conclude that $x^m = x$ for all $x \in w'C$. Write $w' = ah$ where $h \in H$ and choose a dense ideal I of R such that $Ih + hI \subseteq R$. Then $w'I^2w' \subseteq aR \subseteq L$. Clearly $w'I^2w'$ is a nonzero subring of the commutative ring $w'C$. Hence $x^m = x$ for all $x \in w'I^2w'$. Pick any nonzero $y \in w'I^2w'$ and set $w = y^{m-1}$. Obviously

$w^2 = w$, $w \in L$ and $wRw \subseteq w'Hw' = w'C$. Thus $x^m = x$ for all $x \in wRw$ and the proof is complete.

Our final result along these lines is a corollary to Theorem 6.6.2 and Proposition 6.6.4.

Theorem 6.6.5 *Let R be a semiprime ring with extended centroid C, $Q = Q_{mr}(R)$ and $q_1, q_2, \ldots, q_{n+1} \in Q$. We set $e = E(q_1)E(q_2)\ldots E(q_{n+1})$. Suppose $q_1xq_2x\ldots q_nxq_{n+1} = 0$ for all $x \in R$ and $e \neq 0$. Let L be a right (left) ideal of R such that $eL \neq 0$. Then there exist a natural number m and a nonzero idempotent $w \in L$ such that $0 < m < n+1$, wRw is a commutative ring and $x^m = x$ for all $x \in wRw$.*

Proof. Let Φ be the Horn formula given in (6.26) and set $e' = E(\Phi)$. Suppose $e \not\leq e'$. Then there exists $0 \neq f \leq e$ such that $fe' = 0$. Pick $M \in Spec(B)$ such that $f \notin M$. Then $e \notin M$ and so $E(q_i) \notin M$ for all $i = 1, 2, \ldots, n+1$. By Remark 3.2.2 each $\phi_M(q_i) \neq 0$ and we have

$$\phi_M(q_1)x\phi_M(q_2)\ldots x\phi_M(q_{n+1})$$

is a nonzero GPI on $\phi_M(Q)$. By Theorem 6.6.2 $|\phi_M(C)| \leq n$. We note that $\phi_M(Q) \models \Phi$ and see by Theorem 3.2.10 that $e' = E(\Phi) \notin M$. We then have the contradiction $fe' = 0 \in M$, $f \notin M$, $e' \notin M$, and so we conclude that $e \leq e'$. Now let L be a right (left) ideal of R such that $eL \neq 0$. It follows that $e'L \neq 0$ (noting that $e' = E(\Phi)$ is precisely the central idempotent obtained in the proof of Proposition 6.6.4). The conclusion then follows from Proposition 6.6.4

The following result extends to prime rings a theorem originally proved by Slater for primitive rings [266]. The latter result is noteworthy since it was one of the very first results in GPI theory (slightly predating the fundamental theorem of Amitsur [3]).

Theorem 6.6.6 *Let R be a prime ring with extended centroid C, $0 \neq p(x_1, x_2, \ldots, x_n) \in C{<}X{>}$ and $a \in R$. Suppose that $p(a, x_2, x_3, \ldots, x_n)$ is a GPI on R. Then a is algebraic over C.*

Proof. Let A be the central closure of R and $n = \deg_{x_1} p(x)$ Suppose that a is not algebraic over C. Then $p(a, x_2, \ldots, x_n) \neq 0$. Hence R is GPI. According to the prime GPI theorem A is a primitive ring with nonzero socle whose associated division ring is a finite dimensional C-algebra. By Corollary 6.5.13 $\{1, a, a^2, \ldots, a^n\}$ is a C-dependent set modulo $Soc(A)$, whence there exists an element $0 \neq b = \sum_{i=0}^{n} \beta_i a^i \in Soc(A)$, $\beta_i \in C$. By Litoff's Theorem there exists an idempotent $e \in Soc(A)$ such that $b \in eAe$ and $\dim_C(eAe) < \infty$. Thus b (and so a) is algebraic over C.

A standard application of the method of orthogonal completion (Theorem 3.2.18) together with the above theorem yields

Theorem 6.6.7 *Let R be a semiprime ring with extended centroid C, $p(x_1, x_2, \ldots, x_n) \in C{<}X{>}$ and $a \in R$. Suppose that $p(a, x_2, x_3, \ldots, x_n)$ is a GPI on R and at least one coefficient of $p(x)$ equals 1. Then a is algebraic over C.*

Our final application in this chapter gives equivalent conditions for an involution to be symplectic.

Theorem 6.6.8 *Let R be a prime ring ($char(R) \neq 2$) with involution $*$, extended centroid C and central closure $A = RC$. Then the following conditions are equivalent:*

(i) A is a primitive ring with nonzero socle and $*$ is of symplectic type;

(ii) There exists a nonzero element $a \in R$ such that $axx^*a^* = 0$ for all $x \in R$;

(iii) There exists a nonzero element $a \in R$ such that $axa^* + ax^*a^* = 0$ for all $x \in R$.

Proof. (i) $\Rightarrow$ (ii) Since $*$ is of symplectic type, A contains a minimal idempotent e such that $ee^* = 0$. We claim that $exx^*e^* = 0$ for all $x \in A$. Indeed, by Kaplansky's Theorem there exists a vector space ${}_CV$ over a field C with a nondegenerate alternate form $\langle\ ,\ \rangle$ such that $\mathcal{F}_V \subseteq A \subseteq \mathcal{L}_V$ and $*$ is the adjoint map relatively to $\langle\ ,\ \rangle$ (see Theorem 4.6.8). Pick $0 \neq v \in V$ such that $ve = v$. Clearly $V = Cv \oplus V(1-e)$. Let $u, w \in V$. Then $u = \lambda v + u'(1-e)$ and $w = \mu v + w'(1-e)$ for some $\lambda, \mu \in C$ and $u', w' \in V$. We have

$$\langle u,\ wexx^*e^* \rangle = \langle uex,\ wex \rangle = \lambda\mu \langle vx,\ vx \rangle = 0$$

because $\langle t,\ t \rangle = 0$ for all $t \in V$. Since $\langle\ ,\ \rangle$ is nondegenerate, $wexx^*e^* = 0$ for all $w \in V$ and so $exx^*e^* = 0$. Pick any $r \in R$ such that $0 \neq re \in R$. Setting $a = re$ we conclude that $axx^*a^* = 0$ for all $x \in R$.

(ii) $\Rightarrow$ (i) By Theorem 6.2.3 R is GPI and so by the prime GPI theorem A is a primitive ring with nonzero socle. By Kaplansky's Theorem $*$ is either of transpose type or of symplectic type. Suppose $*$ is of transpose type. Then there exists a vector space ${}_\Delta V$ over a division ring Δ with a nondegenerate Hermitian form $\langle\ ,\ \rangle$ such that $\mathcal{F}_V \subseteq A \subseteq \mathcal{L}_V$ and $*$ is the adjoint map relatively to $\langle\ ,\ \rangle$ (see Theorem 4.6.8). Pick $v \in V$ such that $va \neq 0$. Clearly $vaA = V$. Since $\langle\ ,\ \rangle$ is Hermitian, there exists $x \in A$ such that $\langle vax,\ vax \rangle \neq 0$. Then

$$0 \neq \langle vax,\ vax \rangle = \langle v,\ vaxx^*a^* \rangle = 0,$$

a contradiction. Thus $*$ is of symplectic type.

(ii) $\Rightarrow$ (iii) Linearizing the $*$-identity axx^*a^* we obtain that $axy^*a^* + ayx^*a^*$ is a $*$-identity of R. By Theorem 6.4.7 $axy^*a^* + ayx^*a^*$ is a $*$-identity of $Q_s(R)$. Substituting $1 \in Q_s(R)$ for y we conclude that $axa^* + ax^*a^*$ is a $*$-identity of R.

(iii) $\Rightarrow$ (ii) Substituting xx^* for x we obtain $2axx^*a^*$ is a $*$-identity of R. Since $char(R) \neq 2$, axx^*a^* is a $*$-identity of R.

Theorem 6.6.2 was proved by Posner and Schneider [243] in the case of primitive rings with nonzero socle. Corollary 6.6.3 is due to Richoux [249] and Herstein and Small [125].

Chapter 7

T-identities of Prime Rings

7.1 The Home of T-identities

We come now to one of the central topics of this book. Our aim is to give a rigorous and detailed account of the powerful results of Kharchenko concerning prime rings satisfying identities involving derivations and automorphisms (and of the extension of his work by Chuang to include antiautomorphisms). The first order of business is to carefully define these identities, and there are several approaches one can take.

One approach is to naively say that an identity is simply an expression involving fixed ring elements and variables superscripted by composites of derivations and (anti)automorphisms which is sent to zero when the variables are replaced by arbitrary ring elements. But questions about the precise nature of "expressions" and "superscripted variables" quickly indicate the lack of rigor in this simplistic approach. Before describing more acceptable approaches we must first set in place some necessary terminology.

Throughout this chapter R will be a prime ring, C its extended centroid, Φ the prime subfield of C, Q the symmetric ring of quotients of R, D_i the inner derivations of Q, $D = Der(R)C + D_i$, G_i the X-inner automorphisms of R, and $G = Aut(R) \cup Antiaut(R)$. We let G_0 denote a set of representatives of G modulo G_i, and let

$$Aut_0(R) = G_0 \cap Aut(R) \quad \text{and} \quad Antiaut_0(R) = G_0 \cap Antiaut(R).$$

Furthermore we let V be a vector space over C and let X be a C-basis for V, recalling that $C{<}X{>}= C\{V\}$. We have seen in earlier chapters that C, D, and G are all contained in $End_\Phi(Q)$, and we let N denote the subring of $End_\Phi(Q)$ generated by C, D, and G.

Keeping in mind that the "home" for GPI's is

$$Q \coprod_C C{<}X{>}= Q \coprod_C C\{V\}$$

it seems reasonable that the framework we are seeking should be of the form $Q \coprod_C A$ where (for temporary purpose) we shall refer to A as a suitable "algebra of variables".

An appealing choice for A (although one which we shall presently reject) is $A = C{<}X^N{>}$ where X^N is simply a suggestive way of writing $X \times N$. The substitutions we allow are of the form $q \mapsto q$, $x \mapsto r$, $r \in Q$, $x^s \mapsto r^s$, $s \in N$. Then an "identity" is an element of $Q \coprod_C C{<}X^N{>}$ which vanishes under all substitutions just described. Although this definition of identity is quite rigorous it has the drawback that there is no uniqueness to writing the elements of N, and so attempts to work in this framework are fraught with ambiguities. For this reason we must reject this approach.

In order to counteract the lack of uniqueness inherent in the approach just described we shall go to the end of the spectrum (so to speak) and construct the algebra of variables A to be as "free" as possible. To this end let $\overline{D}$ denote the set D, $\overline{G}$ the set G, $\Phi{<}\overline{D} \cup \overline{G}{>}$ the free algebra in the set $\overline{D} \cup \overline{G}$ over

Φ, $\overline{T} = C\coprod_C \Phi{<}\overline{D}\cup\overline{G}{>}$, V a vector space over C, $V^{\overline{T}}$ the Cartesian product of V and $\overline{T}$, and $A = C{<}V^{\overline{T}}{>}$. We let $\sigma : \overline{T} \to End_\Phi(Q)$ be the Φ-algebra map given by $c \mapsto c$, $\overline{\delta} \mapsto \delta$, $\overline{g} \mapsto g$, $c \in C$, $\delta \in D$, $g \in G$. Let $\psi : V \to Q$ be any C-space map and let $\widehat{\psi} : C{<}V^{\overline{T}}{>} \to Q$ be the C-algebra map given by $v^t \mapsto \psi(v)^{\sigma(t)}$, $v \in V$, $t \in \overline{T}$. Then the C-algebra map $Q\coprod_C A \to Q$ which simultaneously lifts id_Q and $\widehat{\psi}$ will be called a $\overline{T}$-substitution. The notion of identity we require can now be defined: $\phi \in Q\coprod_C A$ is a *$\overline{T}$-identity* on I (where $0 \neq I \lhd R$) if ϕ mapped to 0 by all $\overline{T}$-substitutions for which $\psi(X) \subseteq I$.

The favorable aspects of this approach are that there are no hidden relations (because of the freedom of its construction), it has a nice algebraic structure, and it is reasonably natural (if one thinks of v^t as a ”variable” v acted on by an ”endomorphism” t). However, it has the considerable disadvantage that $Q\coprod_C A$ contains many types of elements which are ”trivial” $\overline{T}$-identities in the sense that they have no effect on the ring R. To give the reader an accurate view of the extent of this phenomenon we proceed with the following list of ”obvious” identities. Those of type (A) simply reflect the nature of endomorphisms and of $End_\Phi(Q)$ being a left and right C-space:

$$
\begin{aligned}
&(A_1)\ \ (v+w)^t - v^t - w^t;\\
&(A_2)\ \ v^{s+t} - v^s - v^t;\\
&(A_3)\ \ v^{ct} - (vc)^t;\\
&(A_4)\ \ v^{tc} - v^t \cdot c
\end{aligned}
$$

where $v, w \in V$, $s, t \in \overline{T}$, $c \in C$. Those of type (B) reflect the interrelations among C, D, and G. They are of the form v^{sut} where $v \in V$, $s, t, u \in \overline{T}$, and u is one of the following:

$$
\begin{aligned}
&(B_1)\ \ c\overline{g} - \overline{g}c^g;\\
&(B_2)\ \ c\overline{\delta} - (\overline{\delta}c + c^\delta);\\
&(B_3)\ \ \overline{\delta c} - \overline{\delta}c;
\end{aligned}
$$

$$
\begin{aligned}
&(B_4)\ \ \overline{gh} - \overline{g} \cdot \overline{h};\\
&(B_5)\ \ \overline{\delta} \cdot \overline{g} - \overline{g} \cdot \overline{\delta^g}, \quad \text{where} \quad \delta^g = g^{-1}\delta g;\\
&(B_6)\ \ \overline{\delta} + \overline{\mu} - \overline{\delta + \mu};\\
&(B_7)\ \ [\overline{\delta}, \overline{\mu}] - \overline{[\delta, \mu]};\\
&(B_8)\ \ \overline{\delta}^p - \overline{\delta^p} \quad (\text{if} \quad char(R) = p)
\end{aligned}
$$

where $c \in C$, $\delta, \mu \in D$, $g, h \in G$. Those of type (C) arise from the elements of D_i and G_i:

$$
\begin{aligned}
&(C_1)\ \ v^{t\overline{\mu}} - [a, v^t],\ \mu = ad(a) \in D_i,\ a \in Q;\\
&(C_2)\ \ v^{t\overline{h}} - s^{-1}v^t s,\ h = inn(s) \in G_i,
\end{aligned}
$$

where $t \in \overline{T}$, $v \in V$.

Ultimately, however, we are interested in identities which are "nontrivial" in the sense that they have an impact on the ring R. What we are seeking is a "home" for identities whose structure still retains a degree of freedom to make it tractable to work with but is one in which the identities corresponding to the trivial ones (A_1)–(A_4), (B_1)–(B_8) have already "collapsed" to the zero element. Therefore we shall reject the preceding approach.

It is now time to take the positive step of constructing what we feel is the proper "home" for the identities we will be considering. We begin by focusing our attention on U, the universal enveloping ring of the (restricted) differential C-Lie algebra D. At this point the reader should review the remarks concerning D and U made in section 5.5, as we shall feel free to draw upon the terminology and notations given there without further comment.

We proceed to show that there is an action of G on U, and hence the skew group ring $U \propto G$ exists. (That this is possible should come as no surprise in view of the relations (B_1)–(B_5) previously listed.) Indeed, given $g \in G$ we will define $g^\pi : U \to U$ as follows. Consider the diagram:

$$\begin{tikzcd}
D \arrow[rr] \arrow[dr, "f = f_g"'] & & U \arrow[dl] \\
& U &
\end{tikzcd}$$

where $f : \delta \mapsto \delta^g$. We define an automorphism σ of C by $c^\sigma = c^g$ for all $c \in C$. Considering C as a subring of $End_\Phi(Q)$, we have $c^g = g^{-1}cg$ for all $c \in C$. We proceed to check that f is a σ-semilinear differential C-Lie automorphism of D:

(a) $[\delta, \mu]^f = g^{-1}[\delta, \mu]g = [g^{-1}\delta g, g^{-1}\mu g] = [\delta^f, \mu^f]$;

(b) $(\delta c)^f = g^{-1}\delta cg = g^{-1}\delta gg^{-1}cg = \delta^f c^\sigma$;

(c) $\widehat{\delta^f} = \widehat{g^{-1}\delta g} = g^{-1}\widehat{\delta}g = \sigma^{-1}\widehat{\delta}\sigma$;

(d) $(char(C) = p)\ (\delta^p)^f = g^{-1}(\delta^p)\, g = \left(g^{-1}\delta g\right)^p = \left(\delta^f\right)^p$

where $\delta, \mu \in D$, $c \in C$. Therefore by our discussion in section 5.5 there exists a σ-semilinear Φ-algebra automorphism $g^\pi : U \to U$ completing the diagram. One verifies that π is a homomorphism by applying $(g_1g_2)^\pi$ to the generators of U, i.e., to the elements of C and D. We leave the details for the reader.

We let T denote the skew group ring $U \propto G$ just defined. Clearly T is both a left and right C-space. We then form the right C-space $V \otimes_C T$, with scalar multiplication given by

$$(v \otimes t)c = v \otimes tc, \ v \in V, \ t \in T, \ c \in C.$$

We now take our "algebra of variables" to be the tensor algebra $C\{V \otimes T\}$ of the C-space $V \otimes T$ over C.

The ring

$$\mathcal{S}(Q; R) = \mathcal{S}(R) = \mathcal{S} = Q_C\{V \otimes T\} = Q \coprod_C C\{V \otimes T\}$$

will then be the primary point of reference for the remainder of this chapter, and we shall call $\mathcal{S}$ the *setting* of R . (One notes that the elements corresponding to (A_1)–(A_4) are 0 because of the tensor product $V \otimes T$, and those corresponding to (B_1)–(B_8) are 0 because of the nature of U and of T). Of course we want to view elements such as $v \otimes t$ as an "indeterminate v" acted on by t.

We proceed to describe, at first in a rather general way, a substitution process which is compatible with the idea that an arbitrary C-linear mapping out of V completely determines the substitution. Let P by any C-algebra with 1 which contains Q, and let $\gamma : T \to End_\Phi(P)$ be a fixed C-ring map (i.e., $c^\gamma = c$ for all $c \in C$). Now let $\psi : V \to P$ be any C-space map. Then the map: $V \times T \to P$ given by $(v, t) \mapsto \psi(v)^{\gamma(t)}$ is balanced. Indeed,

$$(vc, t) \mapsto \psi(vc)^{\gamma(t)} = [\psi(v)c]^{\gamma(t)}$$

whereas

$$\begin{aligned}(v, ct) \mapsto \psi(v)^{\gamma(ct)} &= \psi(v)^{\gamma(c)\gamma(t)} = \psi(v)^{c\gamma(t)} \\ &= [\psi(v)c]^{\gamma(t)}.\end{aligned}$$

The additive map: $V \otimes_C T \to P$ so determined is in fact C-linear since

$$\begin{aligned}(v \otimes t)c = v \otimes tc \mapsto \psi(v)^{\gamma(tc)} &= \psi(v)^{\gamma(t)c} \\ &= \left[\psi(v)^{\gamma(t)}\right] c.\end{aligned}$$

It can therefore be lifted to a C-algebra map of $C\{V \otimes T\}$ into P in view of Remark 1.2.1. Hence there exists a (necessarily unique) C-algebra map $\widetilde{\psi}$ of $\mathcal{S}$ into P such that $q \mapsto q$ and $v \otimes t \mapsto \psi(v)^{\gamma(t)}$ for all $q \in Q$, $v \in V$, $t \in T$. Such a map will be called the *T-substitution* determined by ψ (relative to $\gamma : T \to End_\Phi(P)$).

For now the particular choice of P and γ we are interested in is $P = Q$ and γ defined as follows. Recall the map $\rho : U \to$

$End_\Phi(Q)$ (see section 5.5) and the inclusion map $G \to End_\Phi(Q)$. The observations $cg = gc^g$ and

$$\rho(\delta)g - g\rho(\delta^g) = \delta g - g\delta^g = 0$$

show that the hypothesis of Lemma 1.1.4 is satisfied, and hence there is a C-ring map $\gamma : T \to End_\Phi(Q)$. Until further notice the term T-substitution will refer to the γ just described.

We are now in a position to define the notion of T-identity. Fix any C-basis X of V. Let I be a nonzero ideal of R. Then an element ϕ of $\mathcal{S}$ is said to be a *T-identity* on I if ϕ is mapped to 0 under all T-substitutions $\tilde{\psi}$ for which $\psi(X) \subseteq I$. It is straightforward to see that the set of all T-identities (the I may vary, of course) is an ideal of $\mathcal{S}$, and we denote this ideal by $\mathcal{G}_T(Q;\, R)$.

The use of the ring $\mathcal{S} = Q_C\{V \otimes T\}$ as the framework for T-identities has the advantage that "basis-free" arguments can be used. On the other hand the tensor product notation may not have an immediate suggestive appeal for denoting a "variable", and so we shall indicate here an alternative but equivalent description. Let $\mathcal{W}$ be any right C-basis of U (we shall in the sequel usually take $\mathcal{W}$ to be the particular PBW basis given in section 5.5). Then

$$\mathcal{W}G = \{wg \mid w \in \mathcal{W},\ g \in G\}$$

is a right C-basis of T which we denote by T_1. Let X be any C-basis of V. Then the set

$$X \otimes T_1 = \{x \otimes t \mid x \in X,\ t \in T_1\}$$

is a C-basis of $V \otimes T$, and we may accordingly write $C\{V \otimes T\}$ as the free algebra $C{<}X \otimes T_1{>}$ (as indicated by Remark 1.2.4). Since the set $X \otimes T_1$ is in one-one correspondence with the Cartesian product X^{T_1} we will the write $C{<}X \otimes T_1{>}= C{<}X^{T_1}{>}$, it being understood that the element x^{wg} means the element

$x \otimes wg$. Therefore we may write $\mathcal{S}$ alternatively as $Q_C{<}X^{T_1}{>}$. If $\psi : X \to Q$ is a set-theoretic map then the unique C-algebra map of $\mathcal{S}$ into Q given by $q \mapsto q$, $x^t \mapsto \psi(x)^{\gamma(t)}$, $q \in Q$, $x \in X$, $t \in T_1$ will be called the T-substitution determined by ψ , and $\phi \in \mathcal{S}$ is a T-identity on I if ϕ is mapped to 0 by all T-substitutions for which $\psi(X) \subseteq I$.

Next, if C is any field we shall replace the usual setting $\mathcal{S}(C;\, C)$ by a simpler setting as follows. First, since the situation will arise when C is the extended centroid of R and we thus have both $\mathcal{S}(C;\, C)$ and $\mathcal{S}(Q;\, R)$ to contend with simultaneously, we shall pick N to be a C-space with basis Λ disjoint from V with basis X. Then

$$\mathcal{S}(C;\, C) = \mathcal{S}(C) = C\{N \otimes T\} = C{<}\Lambda^{T_1}{>}\ .$$

Clearly the commutator ideal I_1 of $\mathcal{S}(C)$ is contained in $\mathcal{G}(C;\, C)$ (the ideal of all T-identities of C). Therefore it is natural to replace $\mathcal{S}(C)$ by the algebra

$$\mathcal{S}_0(C) = C\{N \otimes T(C)\}/I_1$$

which in turn may by identified with the (commutative) polynomial algebra $C[\Lambda^{T_1}]$. Since any T-substitution of $\mathcal{S}(C)$ into C maps I_1 to 0 it induces a well-defined C-algebra map $\mathcal{S}_0 \to C$, which we continue to refer to as the T-substitution determined by $\psi : N \to C$. Accordingly a T-identity on C will mean any element of $\mathcal{S}_0(C)$ mapped to 0 by all T-substitutions.

Finally, when we study the structure of T-identities in section 7.7, it will be useful to have available the *extended setting* of R

$$\mathcal{S}(Q;\, R) = \mathcal{S}_1(R) = \mathcal{S}_0(C) \otimes_C \mathcal{S}(R).$$

More will be said about $\mathcal{S}_1(R)$ in section 7.3.

7.2 Trivial and Reduced T-identities

We continue to assume R is a prime ring together with the terminology developed in the preceding section. Again we suggest that the reader review section 5.5 since we will feel free to use any remarks and notations made there without further comment.

In section 7.1 we set the stage for the study of T-identities of R by defining the setting $\mathcal{S}$ for R in two equivalent formulations

$$\mathcal{S} = Q_C\{V \otimes_C T\} = Q_C{<}X^{T_1}{>}$$

where V is a C-space with C-basis X, $T = T(R) = U \propto G$ with right C-basis $T_1 = \mathcal{W}G$, $\mathcal{W}$ a PBW right C-basis of U. Since the elements of $\mathcal{S}$ corresponding to the trivial identities (A_1)–(A_4), (B_1)–(B_8) listed in the preceding section are all equal to the zero element of $\mathcal{S}$ we define the set I_0 *of trivial T-identities of* R to be the ideal of $\mathcal{S}$ generated by all elements of the following two forms:

$$\begin{aligned}&(C_1') \;\; v \otimes t\mu - [a, v \otimes t], \;\mu = ad(a) \in D_i;\\ &(C_2') \;\; v \otimes th - s^{-1}(v \otimes t)s, \;h = inn(s) \in G_i\end{aligned}$$

where $v \in V$, $t \in T$.

It will also be useful to have an alternate formulation of I_0. In fact, we claim that I_0 is the ideal of $\mathcal{S}$ generated by all elements of the following forms

$$\begin{aligned}&(C_1'') \;\; x \otimes \Delta g\mu - [a, x \otimes \Delta g], \;\mu = ad(a) \in D_i;\\ &(C_2'') \;\; x \otimes \Delta gh - s^{-1}(x \otimes \Delta g)s, \;h = inn(s) \in G_i\end{aligned}$$

where $x \in X$, $\Delta \in \mathcal{W}$, $g \in G$. Indeed, we may assume without loss of generality that a generator of type (C_1') has the form $xc \otimes \Delta g\mu - [a, xc \otimes \Delta g]$. We note that $xc \otimes \Delta g = x \otimes c\Delta g$. Using the formula (5.25) from section 5.5 we may write

$$c\Delta g = \sum_s \Delta_s g c_{\Delta g s}, \;\Delta_s \in \mathcal{W}.$$

Therefore we may furthermore assume the generator is of the form $x \otimes \Delta g\mu - [a, x \otimes \Delta g]$ (since $c\mu = \mu c$), which is of the desired one. A similar argument works for generators of type (C_2'), and so our claim is established.

We now take T_1 to be the right C-basis of T dictated by the basis $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_i$ of D (see section 5.5) and the representatives G_0 of G modulo G_i. Thus $T_1 = \mathcal{W}G = \mathcal{W}_0\mathcal{W}_iG_0G_i$, where $\mathcal{W} = \mathcal{W}_0\mathcal{W}_i$ is a PBW basis of U, $\mathcal{W}_i$ a PBW basis of $U_i = U(D_i)$.

It will be useful in the sequel to "translate" the basis $\mathcal{B}$ of D and the set of representatives G_0 in the following manner: given $h \in G$ we set $\mathcal{B}^h = \{\delta^h \mid \delta \in \mathcal{B}\}$ and $h^{-1}G_0 = \{h^{-1}g \mid g \in G_0\}$.

Lemma 7.2.1 *(i) $\mathcal{B}_0^h$ is a right C-basis for D modulo D_i;*
(ii) $\mathcal{B}_i^h$ is a right C-basis for D_i;
(iii) $h^{-1}G_0$ is a set of representatives of G modulo G_i.

Proof. Suppose $\sum \delta_j^h c_j = ad(a) \in D_i$, $\delta_j \in B_0$, $c_j \in C$. Writing

$$\sum \delta_j^h c_j = \sum h^{-1}\delta_j h c_j = h^{-1}\left(\sum \delta_j c_j^{h^{-1}}\right) h$$

we then obtain $\sum \delta_j c_j^{h^{-1}} = ad(a^{h^{-1}})$, which forces each $c_j^{h^{-1}}$, and hence each c_j, to equal zero. Next, given $\delta \in D$, we may write

$$\begin{aligned} \delta &= \left(\delta^{h^{-1}}\right)^h = \left(\sum \delta_j c_j\right)^h = \sum h^{-1}\delta_j c_j h \\ &= \sum h^{-1}\delta_j h h^{-1} c_j h = \sum \delta_j^h c_j^h. \end{aligned}$$

Together these remarks prove **(i)**. A similar argument, along with the observation that if $\mu = ad(a)$, then $\mu^h = ad(a^h)$, establishes **(ii)**, and the proof of **(iii)** is immediate.

The bijection between $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_i$ and $\mathcal{B}^h = \mathcal{B}_0^h \cup \mathcal{B}_i^h$ given in Lemma 7.2.1 of course induces a well-ordering $<^h$ of $\mathcal{B}^h$: $\delta < \mu$ if and only if $\delta^h <^h \mu^h$. We can then form the well-ordered PBW right C-basis $\mathcal{W}^h = \mathcal{W}_0^h\mathcal{W}_i^h$ of U with respect to $(\mathcal{B}^h, <^h)$.

We now state our aim in this section: to show that $\mathcal{S}$ is the (semi)direct sum of the ideal I_0 of trivial T-identities and the subring $\mathcal{E} = Q_C{<}X^{T_0}{>}$, where $T_0 = \mathcal{W}_0 G_0$. We shall refer to $\mathcal{E}$ as the subring of *reduced* elements of $\mathcal{S}$ *relatively to* $(\mathcal{B}, <)$.

Our first step toward this goal is to note that since $c \in C$, $\delta = ad(a) \in D_i$, and $inn(s) \in G_i$ are each elements of $End_C(\mathcal{S})$ it follows from Lemma 1.1.4 that there is a C-algebra map $\rho : T_i \to End_C(\mathcal{S})$ where $T_i = U_i \propto G_i \subseteq U \propto G = T$ extending $\alpha : D_i \to End_C(\mathcal{S})$ and $\beta : G_i \to End_C(\mathcal{S})$.

Next we claim that $\mathcal{W}_0 G_0$ is a right T_i-basis of T. Indeed, $\mathcal{W}_0 \mathcal{W}_i G_0 G_i$ is a right C-basis of T and the equation $\Gamma g = g\Gamma^g$, $\Gamma \in \mathcal{W}_i$, $g \in G_0$, shows that $\mathcal{W}_0 \Gamma_0$ generates T as right T_i-module. Now suppose that

$$\sum_{\Delta, g} \Delta g \Omega_{\Delta g} = 0, \ \Delta \in \mathcal{W}_0, \ g \in G_0, \ \Omega_{\Delta g} \in T_i.$$

Using the fact that $\mathcal{W}_i^g$ is a right C-basis of $U_i = U(D_i)$ we write $\Omega_{\Delta g} = \sum w^g h c_{\Delta g w h}$, whence

$$0 = \sum \Delta g \Omega_{\Delta g} = \sum \Delta g w^g h c_{\Delta g w h} = \sum \Delta w g h c_{\Delta g w h},$$

where the summation runs over $\Delta \in \mathcal{W}_0$, $g \in G_0$, $w \in \mathcal{W}_i$, $h \in G_i$. Thus $c_{\Delta g w h} = 0$ and so each $\Omega_{\Delta g} = 0$, which establishes the claim.

We proceed to define a C-space map $\Psi : V \otimes T \to \mathcal{S}$. In preparation for this we again recall the commutation formula

$$c\Delta = \sum_s \Delta_s c^{\widehat{\Delta_{s'}}}, \ \Delta, \Delta_s, \Delta_{s'} \in \mathcal{W}_0, \ c \in C$$

(see (5.25) in section 5.5 for details). From this we see that, for $c \in C$, $\Delta \in \mathcal{W}_0$, $g \in G_0$,

$$c\Delta g = \sum_s \Delta_s g c_{\Delta g s},$$

where $c_{\Delta gs} = c^{\widehat{\Delta_{s'} g}}$. We now claim that the map from $V \times T$ to $\mathcal{S}$ sending $(v, \sum \Delta g \Omega_{\Delta g})$ to $\sum (v \otimes \Delta g)^{\rho(\Omega_{\Delta g})}$ is balanced. Indeed, on the one hand

$$\begin{aligned}
(vc, \sum \Delta g \Omega_{\Delta g}) &\mapsto \sum (vc \otimes \Delta g)^{\rho(\Omega_{\Delta g})} \\
&= \sum (v \otimes c\Delta g)^{\rho(\Omega_{\Delta g})} \\
&= \sum_{\Delta, g, s} (v \otimes \Delta_s g c_{\Delta gs})^{\rho(\Omega_{\Delta g})} \\
&= \sum_{\Delta, g, s} (v \otimes \Delta_s g)^{\rho(c_{\Delta gs} \Omega_{\Delta g})}.
\end{aligned}$$

On the other hand

$$\begin{aligned}
(v, c \sum \Delta g \Omega_{\Delta g}) &= (v, \sum_{\Delta, g, s} \Delta_s g c_{\Delta gs} \Omega_{\Delta g}) \\
&\mapsto \sum_{\Delta, g, s} (v \otimes \Delta_s g)^{\rho(c_{\Delta gs} \Omega_{\Delta g})}.
\end{aligned}$$

We therefore have an additive map $\Psi : V \otimes T \to \mathcal{S}$, and one easily sees that Ψ is a C-space map.

Ψ can be lifted to a C-algebra map of $C\{V \otimes T\}$ into $\mathcal{S}$, and this map together with the inclusion map of Q into $\mathcal{S}$ can be lifted simultaneously to a C-algebra map $\psi : \mathcal{S} \to \mathcal{S}$. Any element of the form $v \otimes t$, $v \in V$, $t \in T$, can be written as a sum of elements of the form $x \otimes \Delta g \Omega$, $x \in X$, $\Delta \in \mathcal{W}_0$, $g \in G_0$, $\Omega \in T_i$. Since it is easily seen that $x \otimes \Delta g \Omega - (x \otimes \Delta g)^{\rho(\Omega)}$ lies in I_0, it follows that $\mathcal{S} = I_0 + \mathcal{E}$. Furthermore the generators (C_1') and (C_2') of I_0 are clearly sent to zero by ψ, and so $\psi(I_0) = 0$. However ψ acts as the identity map on $\mathcal{E}$, whence $I_0 \cap \mathcal{E} = 0$ and $\mathcal{S} = I_0 \oplus \mathcal{E}$. We have thus proved

Theorem 7.2.2 *Let $\mathcal{S} = Q_C\{V \otimes C\} = Q_C < X^{T_1} >$ be the setting of R, I_0 the ideal of trivial T-identities, and $\mathcal{E}$ the subring $Q_C{<}X^{T_0}{>} \subseteq \mathcal{S}$ where $T_0 = \mathcal{W}_0 G_0$. Then $\mathcal{S} = I_0 \oplus \mathcal{E}$.*

The generators of I_0 are of a particularly nice "linear" form, which makes it easy to decompose various subspaces of $\mathcal{S}$ into trivial and reduced components in a very concrete way. Of special interest to us are certain "linear" subspaces of $\mathcal{S}$. For instance most of the proof of Kharchenko's Theorem in section 7.5 takes place in the (Q,Q)-bimodule $Qx^{T_1}Q$. We are also interested in the situation where only derivations and automorphisms are involved. We therefore set in place the following terminology: $G^* = Aut(R)$, $T^* = U \propto G^* \subseteq T$, $G_0^* = G_0 \cap G^*$, $T_1^* = \mathcal{W}G^*$, $T_0^* = \mathcal{W}_0 G_0^*$. We also recall (from the first part of the proof of Theorem 7.2.2) the C-algebra map $\rho : T_i \to End_C(\mathcal{S})$ extending the maps $\alpha : D_i \to End_C(\mathcal{S})$ and $\beta : G_i \to End_C(\mathcal{S})$.

Let us denote by Z the set of generators of I_0 (given in the form (C_1'') and (C_2'')):

$$x \otimes t\mu - [a, x \otimes t],\ x \otimes th - s^{-1}(x \otimes t)s$$

$x \in X$, $t \in T$, $\mu = ad(a) \in D_i$, $h = inn(s) \in G_i$. We set $Z^* = \{z \in Z \mid t \in T_1^*\}$, $Z_x = \{z \in Z \mid x \quad \text{is fixed}\}$, and $Z_x^* = Z^* \cap Z_x$. As we have already noted in the proof of Theorem 7.2.2, any variable $v \otimes t$ is a sum of variables of the form $x \otimes \Delta g \Omega$, $x \in X$, $\Delta \in \mathcal{W}_0$, $g \in G_0$ (or G_0^* if no automorphisms are involved), $\Omega \in T_i$. As a corollary of Theorem 7.2.2 we may then conclude from writing

$$x \otimes \Delta g \Omega = x \otimes \Delta g \Omega - (x \otimes \Delta g)^{\rho(\Omega)} + (x \otimes \Delta g)^{\rho(\Omega)}$$

that the following decompositions into T-trivial and reduced components hold.

Corollary 7.2.3 *(i)* $QX^{T_1}Q = QZQ \oplus QX^{T_0}Q$;
(ii) $QX^{T_1^*}Q = QZ^*Q \oplus QX^{T_0^*}Q$;
(iii) $Qx^{T_1}Q = QZ_xQ \oplus Qx^{T_0}Q$;
(iv) $Qx^{T_1^*}Q = QZ_x^*Q \oplus Qx^{T_0^*}Q$.

Finally, let $\mathcal{S}^* = Q_C{<}X^{T_1^*}{>}$, $\mathcal{E}^* = Q_C{<}X^{T_0^*}{>}$, and I_0^* the ideal of $\mathcal{S}^*$ generated by Z^*. Since $\mathcal{S}^*$ is generated as a ring by $QX^{T_1^*}Q$, Corollary 7.2.3(**ii**) together with Theorem 7.2.2 imply

Corollary 7.2.4 $\mathcal{S}^* = I_0^* \oplus \mathcal{E}^*.$.

7.3 Related Rings

Let R be a prime ring with extended centroid C. Henceforth we may frequently abbreviate ”centrally closed” as ”closed”. In section 7.1 we introduced several rings related to R and C:

$$\begin{aligned} \mathcal{S}(R) &= Q_C\{V \otimes_C T(R)\}, \quad \text{(the setting of } R\text{)}, \\ \mathcal{S}_0(C) &= C[\Lambda^{T(C)}], \quad \text{(the setting of } C\text{), and} \\ \mathcal{S}_1(R) &= \mathcal{S}_0 \otimes_C \mathcal{S}(R) \quad \text{(the extended setting of } R\text{)}. \end{aligned}$$

By Corollary 1.4.11, Theorem 2.3.5, and Theorem 2.4.4, each of these rings is a prime C-algebra with 1, with $\mathcal{S}(R)$ closed over C (i.e, its extended centroid is equal to C). If P denotes any one of these rings we shall be interested in considering $T(P)$ (in case P is closed) or $End_\Phi(P)$ (in any case). Both $T(P)$ and $End(P)$ are C-rings. The important connection we shall make between R and any of these rings P will be to define certain C-ring maps from $T(R)$ to $T(P)$ or $End_\Phi(P)$ which preserve a sufficient part of the structure. Our primary motivation is the need later on for making T-substitutions into larger rings than Q. For instance, in section 7.4 we will need to make the substitution $x \mapsto xd$, $d \in Q$, of X into $\mathcal{S}$. In section 7.7 it will prove useful to make the substitution of X into $\mathcal{S}_1$ given by $x \mapsto x + \lambda y$, $x, y \in X$, $\lambda \in \Lambda$.

We begin by translating Lemma 1.1.4 to our present context.

Lemma 7.3.1 *Let A be a C-ring with* 1, *let $\alpha : D(R) \to A$ be a differential C-Lie algebra map, and let $\beta : G(R) \to A$ be a* *group homomorphism into the units of A. Suppose*

$$\begin{aligned} cg^\beta &= g^\beta c^g, \quad i.e., \quad c^{g^\beta} = c^g && (7.1)\\ \delta^\alpha g^\beta &= g^\beta (\delta^g)^\alpha, \quad i.e., \quad (\delta^\alpha)^{g^\beta} = (\delta^g)^\alpha && (7.2)\end{aligned}$$

for all $c \in C$, $g \in G$, $\delta \in D$. Then α and β may be uniquely extended to a C-ring map $\gamma : T(R) \to A$.

Proof. We know (from the definition of $U(D)$) that α may be extended to a C-ring map of $U(D)$ into A. Since $U(D)$ is generated as a ring by $D(R) \cup C$, we see by Lemma 1.1.4 that α and β may be uniquely extended to a C-ring homomorphism of $T(R)$ into A.

Let P be a closed prime algebra over C. $D(P)$ and $G(P)$ are primarily subsets of $End_\Phi(P)$. They are also embedded in $T(P)$ (with some abuse of notation we have been writing them as being contained in $T(P)$), but some care must be exercised when considering situations where $T(P)$ and $End_\Phi(P)$ are being discussed simultaneously. For instance, an equation involving the elements of $D(P)$ and $G(P)$ may hold in $End_\Phi(P)$ whereas the corresponding equation in $T(P)$ need not hold. Fortunately, because of the special nature of equations (7.1) and (7.2), we have the following useful corollary of Lemma 7.3.1.

Corollary 7.3.2 *Let R be a prime ring with extended centroid C and let P be a prime algebra over C. Let $\alpha : D(R) \to Der(P)$ be a differential C-Lie algebra map and $\beta : G(R) \to G(P)$ a group homomorphism. Suppose the equations (7.1) and (7.2) hold in $End_\Phi(P)$. Then:*

(i) *α and β may be uniquely extended to C-ring map $\gamma : T(R) \to End_\Phi(P)$;*

(ii) *If P is furthermore closed over C, then the equations (7.1) and (7.2) also hold in $T(P)$ and α and β may be uniquely extended to a C-ring map $\gamma : T(R) \to T(P)$.*

We now take up the connection between R and $\mathcal{S} = \mathcal{S}(R) = Q_C\{V \otimes T(R)\}$ in the following series of lemmas. We note that $Der(\mathcal{S}) = D(\mathcal{S})$ (see Theorem 2.4.4).

Lemma 7.3.3 *There is a differential C-Lie algebra injection $\alpha : D(R) \to D(S)$ given by $\delta \mapsto \delta^\alpha$ where δ^α sends $q \to q^\delta$ and $v \otimes t$ to $v \otimes t\delta$, $\delta \in D(R)$, $q \in Q$, $v \in V$, $t \in T(R)$. Furthermore a right C-basis $\mathcal{B}(\mathcal{S})$ of $D(S)$ may be chosen so that $\mathcal{B}(R)^\alpha \subseteq \mathcal{B}(\mathcal{S})$, and $\mathcal{B}_0(R)^\alpha \subseteq \mathcal{B}_0(\mathcal{S})$.*

Proof. For $\delta \in D(R)$, with the aid of Corollary 1.2.3, let δ^α be the derivation of $C\{V \otimes T(R)\}$ determined by $c \mapsto c^\delta$ and $v \otimes t \mapsto v \otimes t\delta$. By Remark 1.4.4 the derivation $q \mapsto q^\delta$ and δ^α can be simultaneously lifted to a uniquely determined derivation of $\mathcal{S}$, which we again denote by δ^α. It is then straightforward to verify that $\delta \mapsto \delta^\alpha$ is a differential C-Lie algebra map of $D(R)$ into $D(\mathcal{S})$. That α is injective follows immediately from the fact that $q^{\delta^\alpha} = q^\delta$ for all $q \in Q$. Thus a right C-basis of $D(\mathcal{S})$ may be chosen so as to contain $\mathcal{B}(R)^\alpha$. Next suppose that $\delta^\alpha \in D_i(\mathcal{S})$, that is, $\delta^\alpha = ad(\phi)$ for some $\phi \in \mathcal{S}$. In particular we have $q^\delta = q^{\delta^\alpha} = [\phi, q]$ for all $q \in Q$. We then map $\mathcal{S}$ into Q by sending every variable $x \in X$ to 0 and q to q, $q \in Q$. If a denotes the image of ϕ the preceding equation becomes $q^\delta = [a, q]$, whence $\delta \in D_i(R)$. As a result $\mathcal{B}_0(R)^\alpha$ is a right C-independent set in $D(\mathcal{S})$ modulo $D_i(\mathcal{S})$, and so a basis $\mathcal{B}'(\mathcal{S}) = \mathcal{B}'_0(\mathcal{S}) \cup \mathcal{B}'_i(\mathcal{S})$ of $D(\mathcal{S})$ may be chosen so that $\mathcal{B}_0(R)^\alpha \subseteq \mathcal{B}'_0(\mathcal{S})$.

Lemma 7.3.4 *There is a group injection $\beta : G(R) \to G(\mathcal{S})$ given by $g \mapsto g^\beta$ where g^β sends q to q^g and $v \otimes t$ to $v \otimes tg$, $g \in G(R)$, $q \in Q$, $v \in V$, $t \in T(R)$. Furthermore given a set of representatives $G_0(R)$ of $G(R)$ modulo $G_i(R)$, a set of representatives $G_0(\mathcal{S})$ of $G(\mathcal{S})$ modulo $G_i(\mathcal{S})$ may be chosen such that $G_0(R)^\beta \subseteq G_0(\mathcal{S})$. Finally $(Aut(R))^\beta \subseteq Aut(\mathcal{S})$, and $(Antiaut(R))^\beta \subseteq Antiaut(\mathcal{S})$.*

Proof. For $g \in G(R)$ the additive map of the right C-space $V \otimes T(R)$ determined by $v \otimes t \mapsto v \otimes tg$ is σ-semilinear where σ denotes the automorphism $c \mapsto c^g$ of C. By Corollary 1.2.2 we may extend this map to a σ-endomorphism g^β of $C\{V \otimes T(R)\}$ (resp. σ-antiendomorphism) if $g \in Aut(R)$ (resp. $g \in Antiaut(R)$). Clearly $(g^{-1})^\beta$ is the inverse of g^β and so g^β is a σ-automorphism (resp. σ-antiautomorphism) of $C\{V \otimes T(R)\}$. The (anti)automorphism g of Q is also a σ-(anti)automorphism of the C-ring Q, and so by Remark 1.4.2 and Remark 1.4.3 $g : Q \to Q$ and g^β can be simultaneously extended to an (anti)automorphism of $\mathcal{S}$ which we again denote by g^β. It is easily verified that $g \mapsto g^\beta$ is a group homomorphism of $G(R)$ into $G(\mathcal{S})$ with (as we already know) $Aut(R)^\beta \subseteq Aut(\mathcal{S})$ and $Antiaut(R)^\beta \subseteq Antiaut(\mathcal{S})$. That β is injective follows from the fact that $q^{g^\beta} = q^g$ for all $q \in Q$. Next suppose $g^\beta \in G_i(\mathcal{S})$, that is, $g^\beta = inn(\phi)$ for some unit $\phi \in \mathcal{S}$. In particular we have

$$q^g = q^{g^\beta} = \phi^{-1} q \phi \quad \text{for all} \quad q \in Q.$$

We then map $\mathcal{S}$ into Q by sending every $x \in X$ to 0 and q to q, $q \in Q$. The image a of ϕ is thus a unit in Q and the preceding equation becomes $q^g = a^{-1}qa$, i.e., $g \in G_i(R)$. Consequently, if

$$\left(g_2^\beta\right)^{-1} g_1^\beta = \left(g_2^{-1} g_1\right)^\beta \in G_i(\mathcal{S})$$

for $g_2, g_1 \in G_0(R)$, we have $g_1 = g_2$, and so we can choose $G_0(\mathcal{S})$ such that $G_0(R)^\beta \subseteq G_0(\mathcal{S})$.

Theorem 7.3.5 *Let $\alpha : D(R) \to D(\mathcal{S})$ and $\beta : G(R) \to G(\mathcal{S})$ be the mappings given in Lemma 7.3.3 and Lemma 7.3.4. Then:*

(i) *α and β may be uniquely extended to a C-ring map $t \mapsto t'$ of $T(R) \to End_\Phi(\mathcal{S})$;*

(ii) *α and β may be uniquely extended to a C-ring injection $\gamma : T(R) \to T(\mathcal{S})$ such that $T_0(R)^\gamma \subseteq T_0(\mathcal{S})$.*

Proof. In either **(i)** or **(ii)**, in order to show that α and β can be simultaneously extended, it suffices in view of Corollary 7.3.2 to show that equations (7.1) and (7.2) hold in $End_\Phi(\mathcal{S})$. It is immediate that (7.1) holds since $c^{g^\beta} = c^g$, $c \in C$, by the definition of β. To verify equation (7.2), it suffices to show that (7.2) agrees on the set $Q \cup (V \otimes T(R))$, which generates $\mathcal{S}$ as a ring. Now using the definitions of α and β, we see that

$$\begin{aligned} q^{(g^\beta)^{-1}\delta^\alpha g^\beta} &= q^{(g^{-1})^\beta \delta^\alpha g^\beta} = q^{g^{-1}\delta g} = q^{\delta^g} = q^{(\delta^g)^\alpha}, \\ (v \otimes t)^{(g^\beta)^{-1}\delta^\alpha g^\beta} &= v \otimes t g^{-1}\delta g = v \otimes t\delta^g = (v \otimes t)^{(\delta^g)^\alpha} \end{aligned}$$

for all $\delta \in D(R)$, $g \in G(R)$, $q \in Q$, $v \in V$, $t \in T(R)$. It remains to be shown in **(ii)** that the extension γ of α and β is injective and that $T_0(R)^\gamma \subseteq T_0(\mathcal{S})$. From Lemma 7.3.3 it follows that α induces an injection of $\mathcal{B}(R)$ into some right C-basis $\mathcal{B}(\mathcal{S})$ and so, with the PBW theorem in mind, the PBW basis $\mathcal{W}(R)$ determined by $\mathcal{B}(R)$ is mapped injectively into the PBW basis $\mathcal{W}(\mathcal{S})$ determined by $\mathcal{B}(\mathcal{S})$. Thus γ induces an injection on $U(D(R))$ into $U(D(\mathcal{S}))$ and, since by Lemma 7.3.4 β is an injection, it follows that γ is an injection of $T(R)$ into $T(\mathcal{S})$. Finally, from $\mathcal{B}_0(R)^\alpha \subseteq \mathcal{B}_0(\mathcal{S})$ (Lemma 7.3.3) implying $\mathcal{W}_0(R)^\gamma \subseteq \mathcal{W}_0(\mathcal{S})$ and $G_0(R)^\beta \subseteq G_0(\mathcal{S})$ (Lemma 7.3.4), we conclude that $T_0(R)^\gamma \subseteq T_0(\mathcal{S})$.

We move on now to the connection between R and $\mathcal{S}_0(C)$. For the present purposes it is best to view $\mathcal{S}_0(C)$ in its original form $\mathcal{S}/I_1(C)$, where $I_1(C)$ is the commutator ideal of $\mathcal{S}(C)$, rather than in its alternative form $C[\Lambda^{T_1(C)}]$. The elements of $\mathcal{S}_0(C)$, cosets by nature, will be denoted by $\overline{\phi}$, $\phi \in \mathcal{S}(C)$. Let $\delta \in D(\mathcal{S}(C))$. Since any derivation of a ring leaves the commutator ideal invariant, it follows that δ induces a derivation $\overline{\delta}$ of $\mathcal{S}_0(C)$ by defining: $\overline{\phi} \mapsto \overline{\phi^\delta}$, $\phi \in \mathcal{S}(C)$. We thus have a differential C-Lie algebra map: $D(\mathcal{S}(C)) \to Der(\mathcal{S}_0(C))$. Similarly there is a group homomorphism $G(\mathcal{S}(C)) \to G(\mathcal{S}_0(C))$ given by $g \mapsto \overline{g}$, where $\overline{g}$ sends $\overline{\phi}$ to $\overline{\phi^g}$, $\phi \in \mathcal{S}(C)$. The equations (7.1) and

(7.2) being easily verified, it follows from Corollary 7.3.2 that $\delta \mapsto \overline{\delta}$ and $g \mapsto \overline{g}$ may be simultaneously lifted to a C-ring map: $T(\mathcal{S}(C)) \to End_\Phi(\mathcal{S}_0(C))$. A connecting link between R and $\mathcal{S}_0(C)$ is now indicated by the following

$$\begin{aligned} D(R) &\to D(C) \to D(\mathcal{S}(C)) \to Der(\mathcal{S}_0(C)), && (7.3)\\ G(R) &\to G(C) \to G(\mathcal{S}(C)) \to G(\mathcal{S}_0(C)), && (7.4)\\ T(R) &\to T(C) \to T(\mathcal{S}(C)) \to End_\Phi(\mathcal{S}_0(C)). && (7.5) \end{aligned}$$

In (7.3) the composite differential C-Lie algebra map will be denoted by $\delta \mapsto \tilde{\delta}$, where $\tilde{\delta}$ sends $\overline{v \otimes \tau}$ to $\overline{v \otimes \tau\delta}$, $v \in N$, $\tau \in T(C)$, $\delta \in D(R)$.

In (7.4) the composite group homomorphism will be denoted by $g \mapsto \tilde{g}$, where $\tilde{g}$ sends $\overline{v \otimes \tau}$ to $\overline{v \otimes \tau g}$.

In (7.5) the composite C-ring map is determined by the mappings in (7.3) and (7.4).

Earlier in this section we have defined a differential C-Lie algebra map $\delta \mapsto \delta'$ of $D(R)$ into $D(\mathcal{S}(R))$, where δ' sends q to q^δ and $v \otimes t$ to $v \otimes t\delta$, $q \in Q$, $v \in V$, $t \in T(R)$. Also we defined a group homomorphism $g \mapsto g'$ of $G(R)$ into $G(\mathcal{S}(R))$, where g' sends q to q^g and $v \otimes t$ to $v \otimes tg$. Together these induce a C-ring map $T(R) \to End_\Phi(\mathcal{S}(R))$.

Now consider the extended setting $\mathcal{S}_1(R) = \mathcal{S}_0(C) \otimes_C \mathcal{S}(R)$. Let $\delta \in D(R)$. By Remark 1.2.9 $\tilde{\delta} : \mathcal{S}_0(C) \to \mathcal{S}_0(C)$ and $\delta' : \mathcal{S}(R) \to \mathcal{S}(R)$ can be uniquely extended to a derivation of $\mathcal{S}_1(R)$ which we denote by δ^α. It is straightforward to verify that α: $D(R) \to Der(\mathcal{S}_1(R))$ is a differential C-Lie algebra map.

By Remark 1.2.7 and Remark 1.2.8 $\tilde{g} : \mathcal{S}_0(C) \to \mathcal{S}_0(C)$ and $g' : \mathcal{S}(R) \to \mathcal{S}(R)$ can be extended to an (anti)homomorphism of $\mathcal{S}_1(R)$ into itself, which we denote by g^β. Clearly $(g^{-1})^\beta$ is the inverse of g^β and so g^β is an (anti)automorphism of $\mathcal{S}_1(R)$. It is easily shown that $\beta : G(R) \to G(\mathcal{S}_1(R))$ is a group homomorphism.

For the maps α and β defined in the preceding paragraph one proceeds to verify the equations (7.1) and (7.2). It suffices to show they agree on ring generators of $\mathcal{S}_1(R)$, namely on elements of the form q ($q \in Q$), $v \otimes \tau$ ($v \in N$, $\tau \in T(C)$), and $v \otimes t$ ($v \in V$, $t \in T(R)$). We leave these details to the reader. Hence by Corollary 7.3.2 we have the following

Remark 7.3.6 *There is a C-ring map $\gamma : T(R) \to End_\Phi(\mathcal{S}_1(R))$ simultaneously extending α and β.*

Finally, let P be any C-algebra with 1 containing Q, and let $\gamma : T(R) \to End_\Phi(P)$ be a C-ring map. By Remark 1.2.6 we have

Remark 7.3.7 *Any T-substitution $\mathcal{S}_0(C) \to C$ and any T-substitution $\mathcal{S}(R) \to P$ (relative to γ) can be uniquely extended to a C-algebra map $\mathcal{S}_1(R) \to P$.*

The import of Remark 7.3.7 is that we can now make T-substitutions involving "central" indeterminates, which will be useful in section 7.7.

7.4 Linear Formulas

In the study of reduced T-identities coming up in section 7.5 the crucial arguments will occur when the T-identity lies in $L_x = Qx^{T_0}Q$. We recall from Corollary 7.2.3(**i**) the decomposition of the (Q,Q)-bimodule

$$Qx^{T_1}Q = QZ_xQ \oplus L_x$$

into its T-trivial and reduced components. Any element $\phi(x) \in L_x$ may be uniquely decomposed as follows

$$\begin{aligned} \phi(x) &= \sum_{g \in G_0} \phi_g(x), \\ \phi_g(x) &= \sum_{\Delta \in \mathcal{W}_0} \phi_{\Delta,g}(x), \qquad (7.6) \\ \phi_{\Delta,g}(x) &\in Qx^{\Delta g}Q. \qquad (7.7) \end{aligned}$$

The support of $\phi(x)$ (briefly, *sup*(ϕ)) consists of all $g \in G_0$ for which $\phi_{\Delta,g}(x) \neq 0$ for some $\Delta \in \mathcal{W}_0$ (or, equivalently, $\phi_g \neq 0$). The set of all such Δ being finite (given ϕ and g) and $\mathcal{W}_0$ being linearly ordered, there exists a unique largest such Δ; we call it the *leading g-term* and denote it by $\Delta_{\phi,g}$.

We next define a useful partial ordering $<$ for L_x which has the property that every nonempty subset S of L_x contains a least element ϕ (in the sense that if $\psi \in L_x$ and $\psi < \phi$ then $\psi \notin S$). We define $<$ as follows. For $\phi, \psi \in L_x$ we say that $\phi < \psi$ precisely when either of the following two conditions holds:

(1) *sup*(ϕ) is a proper subset of *sup*(ψ);

(2) *sup*(ϕ) $=$ *sup*(ψ), $\Delta_{\phi,g} \leq \Delta_{\psi,g}$ for all $g \in$ *sup*(ϕ), and $\Delta_{\phi,g} < \Delta_{\psi,g}$ for some $g \in$ *sup*(ϕ).

Otherwise ϕ and ψ are not compatible. Since $\mathcal{W}_0$ is well-ordered it is easily seen that $<$ is indeed a partial well-ordering for L_x.

Remark 7.4.1 *If $\phi_1, \phi_2 \in L_x$ with sup$(\phi_1) \subseteq$ sup(ϕ_2) and $\Delta_{\phi_1,g} \leq \Delta_{\phi_2,g}$ for all $g \in$ sup(ϕ_1), then for $\psi \in L_x$ $\psi < \phi_1$ implies $\psi < \phi_2$.*

Next let $h \in G$ and let $L_x^h = Qx^{T_0^h}Q$, where $T_0^h = \mathcal{W}_0^h(h^{-1}G_0)$ (recall Lemma 7.2.1 and the subsequent discussion for details). L_x^h is endowed with the partial well-ordering $<^h$ based on $(\mathcal{B}_0^h,\ h^{-1}G_0)$ and the C-space isomorphism between L_x and L_x^h given by $x^{\Delta g} \mapsto x^{\Delta^h h^{-1} g}$, $\Delta \in \mathcal{W}_0$, $g \in G_0$, $\Delta^h = h^{-1}\Delta h \in \mathcal{W}_0^h$ is order preserving. In particular we make the important observation that ϕ is a minimal element of a subset S of L_x if and only if ϕ^h is a minimal element of corresponding set S^h in L_x^h.

For future reference we recall from section 2.5 some definitions concerned with the tensor product $Q^\circ \otimes_\Phi Q$. For $\beta = \sum c_k \otimes d_k$ $c_k, d_k \in Q$ we have

$$\begin{aligned} q \cdot \beta &= \sum c_k q d_k,\ q \in Q, \\ \beta^\delta &= \sum c_k^\delta \otimes d_k,\ \delta \in D(R), \\ \beta^g &= \sum c_k^g \otimes d_k,\ g \in G(R). \end{aligned}$$

For $J \in \mathcal{I}(R)$ N_J denotes the subring of $Q^\circ \otimes_\Phi Q$ generated by all elements of the form $r \otimes r'$, $r, r' \in J$.

At this point we recall the C-ring map $t \mapsto t'$ of $T(R)$ into $End_\Phi(\mathcal{S})$ given by Theorem 7.3.5. We let ρ_d denote the T-substitution of $\mathcal{S}$ into $\mathcal{S}$ determined by $x \mapsto xd$ relative to $t \mapsto t'$, $d \in Q$ $t \in T_1$ (all other indeterminates in X are sent to 0). With some abuse of notation, we may sometimes write $\rho_d(\phi)$ as $\phi(xd)$, and it is understood that $(xd)^t$ means $(xd)^{t'}$. Now for $a, b \in Q$, $\Delta \in \mathcal{W}_0$, $g \in G_0$, we have

$$\rho_d(ax^{\Delta g}b) = a(xd)^{(\Delta g)'}b = a(xd)^{\Delta' g'}b.$$

Applying the Leibnitz Formula to $(xd)^{\Delta'}$ we then can write

$$\rho_d(ax^{\Delta g}b) = \begin{cases} ax^{\Delta g}d^g b + \psi(x) & \text{if} \quad g \in Aut_0(R), \\ ad^g x^{\Delta g} b + \psi(x) & \text{if} \quad g \in Antiaut_0(R) \end{cases} \tag{7.8}$$

where $sup(\psi) \subseteq \{g\}$ and $\Delta_{\psi,g} < \Delta$. It follows from (7.8) that ρ_d maps L_x into itself. Clearly the map: $Q \to End_\Phi(L_x)$ given by $d \mapsto \rho_d$ is additive. Fixing $\phi \in L_x$ we then see that the map $d \mapsto \rho_d(\phi)$ of Q into L_x is additive, and from this we obtain an additive map $\tilde{\phi} : Q^\circ \otimes_\Phi Q \to L_x$ given by $d \otimes c \mapsto \rho_d r_c$ where r_c is the right multiplication by c. Clearly $\phi \mapsto \tilde{\phi}$ is additive and so we have a biadditive map: $L_x \times Q^\circ \otimes_\Phi Q \to L_x$ given by $(\phi, \beta) \mapsto \phi \cdot \beta = \tilde{\phi}(\beta)$, $\beta \in Q^\circ \otimes Q$, $\phi \in L_x$. Thus for $\beta = \sum d_k \otimes c_k \in Q^\circ \otimes Q$ and $\phi \in L_x$ we see that

$$\phi \cdot \beta = \sum \rho_{d_k}(\phi)c_k = \sum \phi(xd_k)c_k. \tag{7.9}$$

In particular, for $a, b, c, d \in Q$, $\Delta \in \mathcal{W}_0$, $g \in G_0$ we have

$$(ax^{\Delta g}b) \cdot (d \otimes c) = \rho_d(ax^{\Delta g}b)c \tag{7.10}$$

Together (7.8) and (7.9) imply

$$sup(\phi_g \cdot \beta) \quad \subseteq \quad \{g\}, \tag{7.11}$$

$$\begin{aligned}\Delta_{\phi\cdot\beta,g} &\leq \Delta_{\phi,g}, &(7.12)\\ sup(\phi\cdot\beta) &\subseteq sup(\phi), &(7.13)\\ (\phi\cdot\beta)_g &= \phi_g\cdot\beta. &(7.14)\end{aligned}$$

We now look at the special case of (7.9) where $\phi(x) = ax^{\Delta g}b$, $a,b \in Q$, $\Delta \in \mathcal{W}_0$, $g \in Aut_0(R)$, and we set $\beta = \sum d_k \otimes c_k$. Together (7.9) and (7.10) enable us to write

$$\begin{aligned}\phi\cdot\beta &= \sum_k a(xd_k)^{\Delta' g'} bc_k\\ &= \sum_k ax^{\Delta g} d_k^g bc_k + \psi(x)\\ &= ax^{\Delta g}(b\cdot\beta^g) + \psi(x) &(7.15)\end{aligned}$$

where $sup(\psi) \subseteq \{g\}$ and $\Delta_{\psi,g} < \Delta$.

More generally we consider $\phi \in L_x$, $g \in sup(\phi)\cap Aut_0(R)$, set $\Delta = \Delta_{\phi,g}$, and write $\phi_{\Delta,g} = \sum_i a_i x^{\Delta g} b_i$, with $\{a_i\}$ C-independent and $\{b_i\}$ C-independent. Then from (7.15) we obtain the formula

$$(\phi\cdot\beta)_{\Delta,g}(x) = \sum_i a_i x^{\Delta g}(b_i\cdot\beta^g) \qquad (7.16)$$

We thus have a criteria for testing when $\Delta_{\phi\cdot\beta,g} < \Delta_{\phi,g}$, namely

Remark 7.4.2 *Given the above notations $\Delta_{\phi\cdot\beta,g} < \Delta_{\phi,g}$ if and only if $b_i\cdot\beta^g = 0$ for each i.*

The following lemma and its corollary will be of crucial importance in section 7.5.

Lemma 7.4.3 *Let $d \in Q$, $\Delta = \delta_1\delta_2\ldots\delta_n \in \mathcal{W}_0$, and let $s \geq 1$ be the largest subscript such that $\delta_1 = \delta_2 = \ldots = \delta_s$ (necessarily $\delta_s < \delta_{s+1}$, and in case of characteristic p, $s < p$). Then*

$$(xd)^{\Delta'} = x^{\Delta}d + sx^{\Omega}d^{\delta_1} + \psi(x),$$

where $\Omega = \delta_2\delta_3\ldots\delta_n$ and the leading term $\Delta_{\psi,1}$ of ψ is less than Ω.

Proof. We set $\Delta_i = \delta_1 \dots \delta_{i-1}\delta_{i+1} \dots \delta_n$, $i = 1, 2, \dots, n$. For $1 \leq i \leq s$ we see that $\Delta_i = \Omega$, whereas for $s+1 \leq i \leq n$ we have

$$\Delta_i = \delta_1 \dots \delta_s \dots \delta_{i-1}\delta_{i+1} \dots \delta_n < \delta_2\delta_3 \dots \delta_n = \Omega.$$

Now, expanding $(xd)^{\Delta'}$ according to the Leibnitz Formula we may conclude that

$$\begin{aligned}(xd)^{\Delta'} &= x^{\Delta}d + \sum_{i=1}^{n} x^{\Delta_i}d^{\delta_i} + \theta(x) \quad (|\Delta_{\theta,1}| < n-1) \\ &= x^{\Delta}d + sx^{\Omega}d^{\delta_1} + \sum_{i=s+1}^{n} x^{\Delta_i}d^{\delta_i} + \theta(x) \\ &= x^{\Delta}d + sx^{\Omega}d^{\delta_1} + \psi(x) \quad (\Delta_{\psi,1} < \Omega).\end{aligned}$$

The proof is complete.

Corollary 7.4.4 *Let $\phi = ax^{\Delta}b$, $a, b \in Q$, $\Delta = \delta_1\delta_2 \dots \delta_n \in \mathcal{W}_0$, $s = s(\Delta)$ as described in Lemma 7.4.3, $J \in \mathcal{I}(R)$, and $\beta \in N_J$. Then:*

$$\phi \cdot \beta = ax^{\Delta}(b \cdot \beta) + sax^{\Omega}(b \cdot \beta^{\delta_1}) + \rho(x)$$

where $\Omega = \delta_2\delta_3 \dots \delta_n$ and $\Delta_{\rho,1} < \Omega$.

Proof. We set $\beta = \sum d_k \otimes c_k$, $c_k, d_k \in J$. By Lemma 7.4.3

$$(xd_k)^{\Delta'} = x^{\Delta}d_k + sx^{\Omega}d_k^{\delta_1} + \psi_k(x),$$

with $\Delta_{\psi_k,1} < \Omega$. Therefore

$$\begin{aligned}\phi \cdot \beta &= \sum_k \phi(xd_k)c_k = \sum_k a(xd_k)^{\Delta'}bc_k \\ &= \sum_k a\left[x^{\Delta}d_k + sx^{\Omega}d_k^{\delta_1} + \psi_k(x)\right]bc_k \\ &= ax^{\Delta}(b \cdot \beta) + sax^{\Omega}(b \cdot \beta^{\delta_1}) + \rho(x),\end{aligned}$$

where $\Delta_{\rho,1} < \Omega$, and the proof is complete.

7.5 Reduced T-identities

We are now able to attain one of the main goals of this book, namely, to establish the fundamental result of Kharchenko (together with Chuang's generalization) which says that if a prime ring R satisfies a nonzero reduced T-identity then R is GPI (Theorem 7.5.8).

Most of the arguments will take place in the special situation where the T-identity is linear and we shall draw heavily upon the material developed in section 7.4. We first recall from Corollary 7.2.3 various linear settings and their decompositions into T-trivial and reduced components

$$\begin{aligned} QX^{T_1}Q &= QZQ \oplus QX^{T_0}Q, \\ Qx^{T_1}Q &= QZ_xQ \oplus L_x, \ \ L_x = Qx^{T_0}Q \end{aligned}$$

and the particular cases where no antiautomorphisms are involved:

$$\begin{aligned} QX^{T_1^*}Q &= QZ^*Q \oplus QX^{T_0^*}Q, \\ Qx^{T_1^*}Q &= QZ_x^*Q \oplus L_x^*, \ \ L_x^* = Qx^{T_0^*}Q. \end{aligned}$$

It turns out that the proof of the main result (Theorem 7.5.8) ultimately rests on Lemma 6.2.1, which we now restate as

Lemma 7.5.1 *Let $h \in Antiaut(R)$ and let $0 \neq \phi \in QxQ + Qx^hQ$ be a T-identity on some $0 \neq I \triangleleft R$. Then R is GPI.*

Also useful will be the following corollary of Corollary 6.1.3.

Lemma 7.5.2 *Let $g \in G$ and let $\phi \in Qx^gQ$ be a T-identity on some $0 \neq I \triangleleft R$. Then $\phi = 0$.*

Proof. Simply note that $\psi(x) = \phi\left(x^{g^{-1}}\right) \in QxQ$ is a GPI on I^g and apply Corollary 6.1.3.

Lemma 7.5.1, Lemma 7.5.3 and Lemma 7.5.4 will, taken together, show that if there is a nonzero reduced linear T-identity on R then R is GPI (Theorem 7.5.5), which in turn will rather quickly yield Theorem 7.5.8. Along the way sharper results will be obtained in case no antiautomorphisms are involved and $char(R) = 0$.

The following lemma is the crucial step in the proof of Theorem 7.5.8.

Lemma 7.5.3 *Let $\phi \in L_x$ be minimal with respect to the property that $\phi \neq 0$, ϕ is a T-identity on some I, and $sup(\phi) \subseteq \{g, h\}$ for some $g \in Aut_0(R)$ and $h \in Antiaut_0(R)$. Then $\Delta_{\phi,f} = 1$ for each $f \in sup(\phi)$.*

Proof. Without loss of generality we may assume that $g = 1$ (since ϕ is minimal in L_x with the given property if and only if ϕ^f is minimal in L_x^f with the same property; see section 7.4 for the details). Furthermore it suffices to show that $\Delta_{\phi,1} = 1$ (since $\Delta_{\phi,h} = 1$ if and only if $\Delta_{\phi^h,1} = 1$). Suppose $\Delta = \Delta_{\phi,1} \neq 1$. Then we write $\Delta = \delta_1\delta_2 \dots \delta_n \in \mathcal{W}_0$ and set $\Omega = \delta_2\delta_3 \dots \delta_n$.

We claim that without loss of generality we may assume that $\phi_{\Delta,1}(x) = ax^\Delta b$. Indeed, we may write

$$\phi_{\Delta,1} = \sum_{i=1}^{m} a_i x^\Delta b_i$$

with $\{a_i\}$ C-independent and $\{b_i\}$ C-independent, $a_1 \neq 0 \neq b_1$. By Remark 2.5.5 there exists $\beta \in N_I$ such that $b_1 \cdot \beta \neq 0$, $b_i \cdot \beta = 0$, $i > 1$. Now by formula (7.16), with $g = 1$, we have

$$(\phi_{\Delta,1} \cdot \beta) = \sum_i a_i x^\Delta (b_i \cdot \beta) = a_1 x^\Delta (b_1 \cdot \beta).$$

Now $0 \neq \phi \cdot \beta \in L_x$ is a T-identity on I, by (7.13)

$$sup(\phi \cdot \beta) \subseteq sup(\phi) \subseteq \{1, h\},$$

and by (7.12) $\Delta_{\phi\cdot\beta,f} \leq \Delta_{\phi,f}$ for each $f \in sup(\phi \cdot \beta)$. Thus the conditions of Remark 7.4.1 are met, and it follows that $\phi\cdot\beta$ must also be a minimal element of L_x relatively to the given requirements. Our claim is thereby established and we will assume that $\phi_{\Delta,1}(x) = ax^{\Delta}b$ where $a, b \neq 0$.

We now extend $\{a\}$ to C-basis $\{a_\xi \mid \xi \in \Xi\}$ of Q and note that $\{a_\xi x^t \mid t \in T_0,\ \xi \in \Xi\}$ is a right Q-module basis for L_x. We write $\phi(x)$ in terms of this basis, being at this time only interested in those basis elements of the form: $ax^{\cdots\Omega}$ (where $\Omega = \delta_2\delta_3\ldots\delta_n$)

$$\phi(x) = ax^{\Delta}b + \sum ax^{\mu_i\Omega}v_i' + \ldots + ax^{\Omega}w' + \ldots \qquad (7.17)$$

$\delta_1 > \mu_1 > \mu_2 > \ldots \in \mathcal{W}_0$, $v_i', w' \in Q$. At this point we note that $\delta_2 \geq \delta_1 > \mu_i$ and so $s(\mu_i\Omega) = 1$ for all i (see Corollary 7.4.4 for the definition of $s(\Delta)$). Now choose $J \subseteq I$ such that aJ, bJ, $v_i'J$, $w'J$ are all contained in R. (Remark: our eventual aim is to show that $\delta_1 + \sum \mu_i\alpha_i = ad(u)$ for suitable $\alpha_i \in C$ $u \in Q$, which will be a contradiction to $\delta_1, \mu_1, \mu_2, \ldots$ being right C-independent modulo D_i). Let $\beta \in N_J$. We compute $\psi_\beta(x) = (\phi\cdot\beta)(x)$, being only concerned in knowing the terms beginning with ax^{Δ} and ax^{Ω}. Note that $\psi_\beta(x)$ remains a T-identity on I. Applying the full force of Corollary 7.4.4 to (7.17), we see that

$$\begin{aligned}
\psi_\beta(x) &= ax^{\Delta}(b\cdot\beta) + sax^{\Omega}(b\cdot\beta^{\delta_1}) + \ldots \\
&\quad + \sum_i ax^{\Omega}(v_i'\cdot\beta^{\mu_i}) + \ldots + ax^{\Omega}(w'\cdot\beta) + \ldots \\
&= ax^{\Delta}(b\cdot\beta) + \ldots \\
&\quad + ax^{\Omega}\left[sb\cdot\beta^{\delta_1} + \sum_i v_i'\cdot\beta^{\mu_i} + w'\cdot\beta\right] + \ldots
\end{aligned}$$

where $s = s(\Delta) \neq 0$ (recall $s < p$ in case of characteristic p, and $s(\mu_i\Omega) = 1$ for all i). Since s is invertible, we can set $v_i = s^{-1}v_i'$, $w = s^{-1}w'$ and rewrite $\psi_\beta(x)$ as follows:

$$\psi_\beta(x) = ax^{\Delta}(b\cdot\beta) + \ldots$$

$$+sax^{\Omega}\left[b\cdot\beta^{\delta_1}+\sum_i v_i\cdot\beta^{\mu_i}+w\cdot\beta\right]+\ldots \tag{7.18}$$

Now we define $f: JbJ\to R$ as follows:

$$b\cdot\beta\mapsto b\cdot\beta^{\delta_1}+\sum_i v_i\cdot\beta^{\mu_i}+w\cdot\beta,\quad \beta\in N_J.$$

We note that v_i and w as well as b are now fixed elements of Q independent of β, that JbJ is an ideal of R, and that the image of f does indeed lie in R (since bJ, $v_i'J$, $w'J$ and hence v_iJ, wJ all lie in R). To show f is well-defined suppose $b\cdot\beta=0$. But then the leading 1-term of $\psi_\beta(x)$ is less than Δ, which says that $\psi_\beta(x)<\phi(x)$, and so by the minimality of $\phi(x)$ we conclude that $\psi_\beta(x)=0$. In particular we then see from (7.18) that

$$s\left[b\cdot\beta^{\delta_1}+\sum_i v_i\cdot\beta^{\mu_i}+w\cdot\beta\right]=0$$

whence

$$b\cdot\beta^{\delta_1}+\sum_i v_i\cdot\beta^{\mu_i}+w\cdot\beta=0$$

(since s is invertible).

It is straightforward to check that f is a right R-map. Indeed, letting $y\in R$, setting $\gamma=\beta(1\otimes y)$, and noting that

$$\gamma^{\delta}=\beta^{\delta}(1\otimes y),\ \delta\in D(R),$$

we have

$$\begin{aligned} b\cdot\beta y &= b\cdot\gamma\mapsto b\cdot\gamma^{\delta_1}+\sum_i v_i\cdot\gamma^{\mu_i}+w\cdot\gamma \\ &= \left[b\cdot\beta^{\delta_1}+\sum_i v_i\cdot\beta^{\mu_i}+w\cdot\beta\right]y=f(b\cdot\beta)y \end{aligned}$$

Next we set $u=\{f,\ JbJ\}\in Q_r(R)$ and note that

$$u(b\cdot\beta)=f(b\cdot\beta)=b\cdot\beta^{\delta_1}+\sum_i v_i\cdot\beta^{\mu_i}+w\cdot\beta \tag{7.19}$$

for all $\beta \in N_J$. Multiplication of (7.19) on the left by $y \in R$ yields

$$yu(b \cdot \beta) = y(b \cdot \beta^{\delta_1}) + \sum_i y(v_i \cdot \beta^{\mu_i}) + y(w \cdot \beta). \tag{7.20}$$

On the other hand, setting $\gamma = \beta(y \otimes 1)$ and using formula (2.13)

$$\gamma^\delta = \beta^\delta(y \otimes 1) + \beta(y^\delta \otimes 1),$$

we have

$$\begin{aligned} uy(b \cdot \beta) &= u(b \cdot \gamma) = b \cdot \gamma^{\delta_1} + \sum_i v_i \cdot \gamma^{\mu_i} + w \cdot \gamma \\ &= y^{\delta_1}(b \cdot \beta) + y(b \cdot \beta^{\delta_1}) + \sum_i y^{\mu_i}(v_i \cdot \beta) \\ &\quad + \sum_i y(v_i \cdot \beta^{\mu_i}) + y(w \cdot \beta) \end{aligned} \tag{7.21}$$

Subtraction of (7.21) from (7.20) yields

$$(yu - uy)(b \cdot \beta) = y^{\delta_1}(b \cdot \beta) + \sum_i y^{\mu_i}(v_i \cdot \beta) \tag{7.22}$$

for all $y \in R$ and $\beta \in N_J$.

Finally, we extend $\{b\}$ to a C-basis $\{b_\xi \mid \xi \in \Xi\}$ of Q with $b = b_1$. For each i (only a finite number) we write

$$v_i = \sum_j \alpha_{ij} b_j, \quad \alpha_{ij} \in C.$$

This only involves a finite number of b_j's, say, $b = b_1, b_2, \ldots, b_m$. By Remark 2.5.5 we may choose $\gamma \in N_J$ such that $b \cdot \gamma = b_0 \neq 0$ and $b_j \cdot \gamma = 0, j > 1$. We note that $b_0 \in JbJ \subseteq J$. Then, for any $\beta \in N_J$, we use (7.22) to compute

$$\begin{aligned} [y, u](b_0 \cdot \beta) &= [y, u](b \cdot (\gamma\beta)) \\ &= y^{\delta_1}(b \cdot (\gamma\beta) + \sum_i y^{\mu_i}(v_i \cdot (\gamma\beta)) \end{aligned}$$

$$\begin{aligned} &= y^{\delta_1}(b_0\cdot\beta)+\sum_{ij}\alpha_{ij}y^{\mu_i}(b_j\cdot(\gamma\beta)) \\ &= y^{\delta_1}(b_0\cdot\beta)+\sum_{i}\alpha_{i1}y^{\mu_i}((b\cdot\gamma)\cdot\beta) \\ &= y^{\delta_1}(b_0\cdot\beta)+\sum_{i}\alpha_{i}y^{\mu_i}(b_0\cdot\beta) \ \ (\alpha_i=\alpha_{i1}\in C). \end{aligned}$$

Therefore

$$\left(y^{\delta_1}+\sum_i\alpha_i y^{\mu_i}-[y,\,u]\right)(b_0\cdot\beta)=0$$

for all $y\in R$ and $\beta\in N_J$. Hence

$$y^{\delta_1}+\sum_i\alpha_i y^{\mu_i}=[y,\,u]$$

for all $y\in R$, in other words,

$$\delta_1+\sum_i\mu_i\alpha_i=ad(u)\in D_i.$$

This is a contradiction since $\delta_1,\mu_1,\mu_2,\ldots$ are C-independent modulo D_i, and the proof is complete.

The next lemma shows that if there is a nontrivial linear T-identity then the conditions of Lemma 7.5.3 will be fulfilled.

Lemma 7.5.4 *If $\phi\in L_x$ is minimal with respect to the property that $0\neq\phi$ is a T-identity for some $0\neq I\lhd R$, then $sup(\phi)\subseteq\{g,h\}$ for some $g\in Auto_0(R)$ and $h\in Antiauto_0(R)$.*

Proof. If the lemma is false we claim that we may assume without loss of generality that $sup(\phi)$ contains two automorphisms g_1 and g_2. Indeed, if g and h are two antiautomorphisms in $sup(\phi)$, then $sup\,(\phi^g)$ contains the two automorphisms 1 and $g^{-1}h$, and our claim is thereby established. Therefore let g_i,

$i = 1, 2$ be two automorphisms in $sup(\phi)$, and let $\Delta_i = \Delta_{\phi,g_i}$ be the leading g_i-term of ϕ. We write

$$\phi_{\Delta_i,g_i} = \sum_{j=1}^{m_i} a_{ij} x^{\Delta_i g_i} b_{ij}, \quad i = 1, 2$$

with $\{a_{i1}, a_{i2}, \dots, a_{im_i}\}$ C-independent and $\{b_{i1}, b_{i2}, \dots, b_{im_i}\}$ C-independent. We claim that b_{11} is left independent of

$$b_{12}, b_{13}, \dots, b_{1m_1}, b_{21}, b_{22}, \dots, b_{2m_2}$$

with respect to

$$\underbrace{g_1, g_1, \dots, g_1}_{m_1 \text{ times}}, \underbrace{g_2, g_2, \dots, g_2}_{m_2 \text{ times}}.$$

If not we have (in view of Remark 2.5.8)

$$b_{11} \in \sum_{j=2}^{m_1} M_{g_1^{-1}g_1} b_{1j} + \sum_{j=1}^{m_2} M_{g_1^{-1}g_2} b_{2j} = \sum_{j=2}^{m_1} C b_{1j},$$

a contradiction to $b_{11}, b_{12}, \dots, b_{1m_1}$ being C-independent. Now by Theorem 2.5.9 there exists $\beta \in N_I$ such that

$$\begin{aligned} b_{11} \cdot \beta^{g_1} &\neq 0, \quad b_{1j} \cdot \beta^{g_1} = 0, \quad j = 2, 3, \dots, m_1, \\ b_{2j} \cdot \beta^{g_2} &= 0, \quad j = 1, 2, \dots, m_2 \end{aligned}$$

The element $\phi \cdot \beta \in L_x$ is a T-identity on I and, in view of (7.16), $\phi \cdot \beta \neq 0$ since $b_{11}\beta^{g_1} \neq 0$. By the criterion of Remark 7.4.2 we see that $\Delta_{\phi\cdot\beta,g_2} < \Delta_{\phi,g_2}$, whence $\phi \cdot \beta < \phi$ in contradiction to the minimality of ϕ. The proof is thereby complete.

Theorem 7.5.5 *Let $0 \neq \phi \in QX^{T_0}Q$ be a T-identity on some $0 \neq I \triangleleft R$. Then R is GPI.*

Proof. Without loss of generality we may assume that $\phi \in L_x$ for some $x \in X$. Furthermore we may assume that ϕ is a minimal nonzero T-identity on I. Then Lemma 7.5.4, Lemma 7.5.3 and Lemma 7.5.1 together imply that R is GPI.

Theorem 7.5.5 may be improved upon if there are no anti-automorphisms present.

Theorem 7.5.6 *If $\phi \in QX^{T_0^*}Q$ is a T-identity on some $0 \neq I \lhd R$, then $\phi = 0$.*

Proof. We may assume without loss of generality that $\phi \in L_x^*$ and is a minimal nonzero T-identity on I. By Lemma 7.5.4 $sup(\phi) \subseteq \{g, h\}$, $g \in Aut_0(R)$, $h \in Antiaut_0(R)$ and, since $\phi \in L_x^*$, we must in fact have $sup(\phi) \subseteq \{g\}$. By Lemma 7.5.3 $\Delta_{\phi,g} = 1$ and, in view of Lemma 7.5.2, we reach the contradiction that $\phi = 0$.

Before moving on to the general case of a T-identity we shall briefly review the linearization process in $\mathcal{S} = Q_C < X^{T_1} >$. With some obvious adjustments it is basically the same as that described in section 6.1, and the reader can refer to the account given there (preceding Remark 6.1.5). Again we start with the usual monomial basis $\mathcal{M}(\mathcal{A})$ of $\mathcal{S}$. For each $M \in \mathcal{M}(\mathcal{A})$ let $\widehat{M} \in \mathcal{M}(\mathcal{A})$ be obtained by replacing each x^t by x, $x \in X$, $t \in T_1$. Then, if ν represents any of the functions $\deg_x$, deg, ht_x, ht, we define $\nu(M) = \nu(\widehat{M})$. For $\phi = \sum c_M M$ we define $\nu(\phi) = \max_M \nu(M)$ where M belongs to ϕ. As a notational example, if $M \in \mathcal{M}(\mathcal{A})$ is such that $\deg_x(M) = k$, then one may write

$$M = M(x) = P_{i_0}x^{t_1}P_{i_1}x^{t_2}\dots x^{t_k}P_{i_k}$$

where $t_j \in T_1$ and $P_{i_j} \in \mathcal{M}(\mathcal{A})$ containing only variables of the form x_i^t, $x_i \neq x$, $t \in T_1$. Now let $\phi = \phi(x_1, x_2, \dots, x_n) \in \mathcal{S}$. ϕ is *k-homogeneous in x* if $\deg_x(M) = k$ for every M belonging to ϕ, and given a sequence $\tau = (m_1, m_2, \dots, m_n)$ ϕ is *τ-homogeneous* if ϕ is m_i-homogeneous in x_i, $i = 1, 2, \ldots, n$. Clearly any $\psi \neq 0$ may be uniquely written as a sum $\sum \psi_\tau$, ψ_τ τ-homogeneous, or, for a fixed x, $\sum_{k=0}^{m} \psi_k(x)$, $\psi_k(x)$ k-homogeneous in x, $m = \deg_x(\psi)$. We say ϕ is *T-multilinear of degree n* if ϕ is τ-homogeneous with each $m_i = 1$, $i = 1, 2, \ldots, n$.

With this terminology in hand the linearization process proceeds exactly as described in section 6.1. An operation of type A may be used whenever $\deg_x(\phi) > 1$ for some $x \in X$: deg is preserved, height is lowered, and T-identity is preserved. An operation of type B may be used whenever there is an $x \in X$ appearing in some but not all monomials belonging to ϕ: T-identity is preserved, and neither degree nor height is raised. As in section 6.1 every $0 \neq \phi \in S$ has a linearization and so we may state

Remark 7.5.7 *If $0 \neq \phi \in S$ is a reduced T-identity of degree n on some $0 \neq I \triangleleft R$, then there is a nonzero reduced T-multilinear identity of* deg $\leq n$.

We come now to one of the main results in the theory of generalized identities. In the case of derivations and automorphisms it was proved by Kharchenko in 1978, and it was extended to include antiautomorphisms by Chuang in 1990 ([143], [146], [82], [86], [88]).

Theorem 7.5.8 *Let R be a prime ring and let ϕ be a nonzero reduced T-identity on some nonzero ideal I of R. Then R is GPI.*

Proof. The proof is by induction on $n = \deg(\phi)$. The case $n = 1$ is given by Theorem 7.5.5. Now let ϕ be a T-identity of degree n on some $0 \neq I \triangleleft R$. By Remark 7.5.7 we may assume that $\phi = \phi(x_1, x_2, \ldots, x_n)$ is T-multilinear of degree n. Let $r_2, r_3, \ldots, r_n \in I$ and let $\psi(x_1) = \phi(x_1, r_2, r_3, \ldots, r_n)$ be the image of ϕ under the T-substitution $x_1^t \mapsto x_1^t$, $x_i^t \mapsto r_i^{\gamma(t)}$, $t \in T_0$, $i = 2, 3, \ldots, n$, relative to the mapping $\gamma : T \to$

$End_\Phi(S)$ described in section 7.1. We note that $\psi(x_1) \in L_{x_1}$ is a T-identity on I. If $\psi(x_1) \neq 0$ we are again finished by Theorem 7.5.5. Therefore we may assume $\psi(x_1) = 0$ which implies that ψ maps to 0 under the substitution $x_1^t \mapsto r_t \in I$ for any choice $r_t \in I$, $t \in T_0$. Thus the image $\rho = \rho(x_2, \dots, x_n)$ of ϕ under the substitution $x_1^t \mapsto r_t$, $x_i^t \mapsto x_i^t$, $i = 2, 3, \dots, n$ is a T-identity on I of deg $\leq n-1$, and so by induction we may assume that $\rho = 0$. Altogether this shows that ϕ maps to 0 under any substitution $x_i^t \mapsto r_{i,t} \in I$, $t \in T_0$, $i = 1, 2, \dots, n$. Thus we have found a *GPI* $\chi(x_{i,t})$ such that the substitution $x_{i,t} \mapsto x_i^t$ maps it to ϕ. Hence $\chi \neq 0$ and R is *GPI*.

In case $char(R) = 0$ and ϕ is a T-identity without antiautomorphisms we have the following sharper result.

Theorem 7.5.9 *Let $char(R) = 0$ and let*

$$0 \neq \phi = \phi(x_1, x_2, \dots, x_n) \in Q_C{<}X^{T_0^*}{>}$$

be a T-identity on some $0 \neq I \triangleleft R$. Let $\{y_{it}\}$ be distinct elements of X in one-one correspondence with the variables x_i^t. Then $\phi(y_{it})$ is a GPI on Q (it is understood that $\phi(y_{it})$ is mapped to $\phi(x)$ under the substitution $y_{it} \mapsto x_i^t$, $t \in T_0^*$, $1 \leq i \leq n$).

Proof. The proof is by induction on $ht(\phi)$. We first claim that it suffices to assume that ϕ is homogeneous. Indeed, we write $\phi = \sum_{k=0}^m \phi_k$ where ϕ_k is k-homogeneous in x_1, noting that

$$0 = \phi(jr_1, r_2, \dots, r_n) = \sum_{k=0}^{m} j^k \phi_k(r_1, r_2, \dots, r_n)$$

for $j = 1, 2, \dots, m+1$. Since $char(R) = 0$, $1, 2, \dots, m+1$ are distinct elements in the prime field Φ and so, using a Vandermonde determinant argument, each $\phi_k(r_1, r_2, \dots, r_n) = 0$, i.e., ϕ_k is a T-identity on I, $k = 0, 1, \dots, m$. Repeated use of the above argument ultimately shows that we may write $\phi = \sum \phi_\tau$, where each ϕ_τ is a τ-homogeneous T-identity on I. By assumption each ϕ_τ is a GPI on Q whence ϕ is a GPI on Q and the claim is established.

For $ht(\phi) = 0$ we know that $\phi = \phi(x_1, x_2, \ldots, x_n)$ is T-multilinear (since we are assuming ϕ is homogeneous). Let $r_2, r_3, \ldots, r_n \in I$ and set $\psi(x_1) = \phi(x_1, r_2, \ldots, r_n) \in L_x^*$. Since ψ is a T-identity on I we know by Lemma 7.5.2 that $\psi(x_1) = 0$. In particular, for any choice $q_t \in Q$, $t \in T_0^*$, $\phi(x_1, x_2, \ldots, x_n)$ is mapped to 0 by $x_1^t \mapsto q_t$, $x_i^t \mapsto r_i^{\gamma(t)}$, $i = 2, 3, \ldots, n$. Continuing this process with $x_2, x_3, \ldots, x_n$ we see that, given any choice $q_{i,t} \in Q$, $t \in T_0^*$, $i = 1, 2, \ldots, n$, ϕ is mapped to 0 by $x_i^t \mapsto q_{i,t}$. The conclusion of the theorem follows immediately in this case.

We now suppose that $ht(\phi) > 0$. We may assume, say, that $r = \deg_{x_n} > 1$. We then apply an operation of type A in the linearization process, namely, for $y \in X$ distinct from $x_1, x_2, \ldots, x_n$ we replace ϕ by

$$\begin{aligned}\psi(x_1, \ldots, x_n, y) &= \phi(x_1, \ldots, x_{n-1}, x_n + y)\\ &\quad -\phi(x_1, \ldots, x_n) - \phi(x_1, \ldots, x_{n-1}, y)\end{aligned}$$

noting that $ht(\psi) < ht(\phi)$ and ψ is again a T-identity on I. Then the induction hypothesis says that ψ is a GPI on Q. Furthermore, since ϕ is r-homogeneous in x_n we see that

$$\begin{aligned}\psi(x_1, \ldots, x_n, x_n) &= \phi(x_1, \ldots, x_{n-1}, 2x_n) - 2\phi(x_1, \ldots, x_n)\\ &= (2^r - 2)\phi(x_1, x_2, \ldots, x_n)\end{aligned}$$

whence ϕ is a GPI on Q (in a view of $char(R) = 0$). The proof of the theorem is complete.

Under the conditions of Theorem 7.5.9, if ϕ is a T-identity on $0 \neq I \triangleleft R$, one may say, in somewhat looser language, that the variables x_i^t can be "freed" (replaced by $y_{i,t}$) and that the resulting element vanishes on all of Q. In general, if $char(R) = p$ and/or ϕ involves antiautomorphisms, the conclusion of Theorem 7.5.9 is no longer always valid. However, as we shall show in sections 7.6 and 7.7, the variables x_i^t may be "partially" freed and the resulting element will be a T-identity on Q.

7.6 The Structure of T-identities (Fields)

In section 7.5 the central result (Theorem 7.5.8) was that a nonzero reduced T-identity on a nonzero ideal of a prime ring forced the ring to be GPI. However, there was no special effort to keep track of the original T-identity. In the present section and section 7.7 our aim is to prove some results about the T-identities themselves. The case in which $R = C$ is a field, for which we give a complete analysis in this section, is not only used heavily in the general situation of prime rings in the following section, but may be of independent interest in its own right.

Let C be a field. In this special situation we recall from section 7.1 that the setting for C is defined to be the commutative polynomial ring

$$\mathcal{S}_0(C) = C[\Lambda^{T_1(C)}] = C{<}\Lambda^{T_1(C)}{>}/I_1(C)$$

where $I_1(C)$ is the commutator ideal of $C{<}\Lambda^{T_1(C)}{>}$. We recall too in this situation that since $D_i = 0$ and $G_i = 1$, $\mathcal{W} = \mathcal{W}_0$, $G = G_0$ and accordingly $T_1 = \mathcal{W}_0 G_0 = T_0$.

It will prove useful to further refine G as follows. We define an automorphism $g \in G$ to be *Frobenius* if either $g = 1$ or, in case $char(C) = p$ and $\theta : c \mapsto c^p$ is an automorphism, $g = \theta^l$ for some $l \in \mathcal{Z}$. We let G_f denote the set of all Frobenius automorphisms of C and note that G_f is a normal subgroup of G. If $char(C) = 0$ or $char(C) = p$ and θ is *not* onto, then $G_f = 1$. In case $char(C) = p$ and θ is onto then G_f is the cyclic group generated by θ, being infinite (resp. finite) if and only if C

is infinite (resp. finite). We choose a set G_{0f} of representatives of G modulo G_f and accordingly take $G = G_0$ to be $G_{of}G_f = \{g_k f_l \mid g_k \in G_{0f},\ f_l \in G_f\}$. We note in passing that if $G_f \neq 1$, then necessarily $\mathcal{W} = \{1\}$. Indeed, every element of C in this case is a pth power c^p and if $\delta \in Der(C)$, then $(c^p)^\delta = pc^{p-1}c^\delta = 0$. Also, if C is a finite field of order p^n, $G = G_f$ is cyclic of order n (hence $G_{0f} = 1$) and of course $\mathcal{W} = \{1\}$.

With the above decomposition of G in mind it is clear that the set of all finite products

$$M = \prod \left(\lambda_i^{\Delta_j g_k f_l}\right)^{m_{ijkl}}, \quad m_{ijkl} \in \mathcal{N} \qquad (7.23)$$

forms a C-basis of $C[\Lambda^{T_0}]$, where $\mathcal{N} = \{0,1,2,\ldots\}$, $\lambda_i \in \Lambda$, $\Delta_j \in \mathcal{W}$, $g_k \in G_{of}$, $f_l \in G_f$.

In analyzing the T-identities of C it is convenient to consider separate situations which we label as follows:

(1a) $G_f = 1$ and $char(C) = 0$;

(1b) $G_f = 1$ and $char(C) = p > 0$;

(2a) $G_f \neq 1$ and C is infinite (hence G_f is the infinite cyclic group $\{\theta^l \mid l \in \mathcal{Z}\}$ and $\mathcal{W} = \{1\}$);

(2b) $G_f \neq 1$ and C is finite (hence G_f is the finite cyclic group $\{\theta^l \mid l = 0,1,\ldots,n-1\}$ and $\mathcal{W} = \{1\}$).

There are in some cases some "obvious" T-identities of C which we describe as follows.

In cases **(1a)** and **(1b)** there are no other "obvious" T-identities and we set $I_2(C) = 0$.

In case **(2a)** we define $I_2(C)$ to be the ideal of $C[\Lambda^{T_0}]$ generated by all elements of the form

$$\left(\lambda^{g\theta^l}\right)^p - \lambda^{g\theta^{l+1}}, \quad \lambda \in \Lambda,\ g \in G_{0f}$$

where θ is the basic Frobenius automorphism $c \mapsto c^p$, $c \in C$.

In case **(2b)** we define $I_2(C)$ to be the ideal of $C[\Lambda^{T_0}]$ generated by all elements of the form

$$\lambda^{\theta^l} - \lambda^{p^l}, \quad \lambda \in \Lambda,\ l = 1,2,\ldots,n$$

where $|C| = p^n$. We note that

$$\lambda - \lambda^{p^n} = \lambda^{\theta^n} - \lambda^{p^n} \in I_2(C).$$

We shall call $I_2 = I_2(C)$ the ideal of *F-trivial* T-identities of $C[\Lambda^{T_0}]$. Our goal in this section is to show that every T-identity of C is F-trivial.

To this end it is first of all important to determine an explicit C-basis for $C[\Lambda^{T_0}]$ modulo $I_2(C)$. For future reference it will be useful to have a simpler description of the monomials in (7.23) in the various cases **(1a)**, **(1b)**, **(2a)** and **(2b)**:

$$\begin{aligned} M &= \prod \left(\lambda_i^{\Delta_j g_k}\right)^{m_{ijk}}, \\ & \quad m_{ijk} \in \mathcal{N} \quad \text{in cases } \textbf{(1a)} \text{ and } \textbf{(1b)}; \qquad (7.24) \\ M &= \prod \left(\lambda_i^{g_k \theta^l}\right)^{m_{ikl}}, \\ & \quad m_{ikl} \in \mathcal{N},\ l \in \mathcal{Z} \quad \text{in case } \textbf{(2a)}; \qquad (7.25) \\ M &= \prod \left(\lambda_i^{\theta^l}\right)^{m_{il}}, \\ & \quad m_{il} \in \mathcal{N},\ l = 0, 1, \ldots, n-1 \quad \text{in case } \textbf{(2b)}; .(7.26) \end{aligned}$$

We define $N = \mathcal{N}$ (in cases **(1a)** and **(1b)**) and $N = \mathcal{N}_p = \{\sum_{l=-q}^{q} s_l p^l \mid q \in \mathcal{N},\ 0 \le s_l < p\}$ (case **(2a)**).

We next define the important notion of *F-degree* in cases **(1a)**, **(1b)**,**(2a)** and **(2b)**. For a monomial given in (7.23) we define the F-degree of $\lambda_{i_0}^{\Delta_{j_0} g_{k_0}}$ in M by consideration of the three forms of M as shown in (7.24)–(7.26):

$$\begin{aligned} & m_{i_0 j_0 k_0} \quad \text{in cases } \textbf{(1a)} \text{ and } \textbf{(1b)}, \\ & \sum_l m_{i_0 k_0 l} p^l \quad \text{in case } \textbf{(2a)}, \\ & r \quad \text{in case } \textbf{(2b)}, \text{ where} \\ & \quad \sum_l m_{i_0 l} p^l - 1 = q(p^n - 1) + r_0, \\ & \quad 0 \le r_0 < p^n - 1,\ r = r_0 + 1. \end{aligned}$$

We remark that in cases **(1a)** and **(1b)** the F-deg of $\lambda^{\Delta g}$ in M is just the ordinary degree of the variable $\lambda^{\Delta g}$ in M. In case **(2a)** we note that F-deg of λ^{g} in M need not be an integer (if $l < 0$). In all cases the notion of F-deg is quite natural if one thinks of it as the "power" to which $\lambda^{\Delta g}$ occurs in M when θ^{l} is replaced by p^{l}. Finally if

$$\phi = \sum_{M} c_M M, \quad c_M \in C, \ M \quad \text{of form (7.23)}$$

is an arbitrary element of $C[\Lambda^{T_0}]$ we define:

$$F\text{-deg of } \lambda^{\Delta g} \text{ in } \phi = \max\{F\text{-deg of } \lambda^{\Delta g} \text{ in } M\}.$$

Again we remark that if $G_f = 1$, then the F-deg of $\lambda^{\Delta g}$ in ϕ coincides with the ordinary degree of $\lambda^{\Delta g}$ in ϕ.

We consider now the Cartesian product $\Lambda \times \mathcal{W} \times G_{0f}$, a typical element of which will be denoted by $\alpha = (\lambda_i, \Delta_j, g_k)$ (with $\alpha_1 = \lambda_i$, $\alpha_2 = \Delta_j$, $\alpha_3 = g_k$), and mappings

$$s : \Lambda \times \mathcal{W} \times G_{0f} \to N,$$

it being understood that s always has finite support, i.e., $s(\alpha) \neq 0$ for only a finite number of α's. Using these notations we next define certain monomials

$$V_{\alpha,s} = \begin{cases} \left(\lambda_i^{\Delta_j g_k}\right)^{s(\alpha)}, & \text{in cases } \mathbf{(1a)} \text{ and } \mathbf{(1b)}, \\ \prod_l \left(\lambda_i^{g_k \theta^l}\right)^{s_l(\alpha)}, & s(\alpha) = \sum_l s_l(\alpha) p^l,\ 0 \leq s_l(\alpha) < p, \\ & \text{in case } \mathbf{(2a)}, \\ \lambda_i^{s(\alpha)}, & 0 \leq s(\alpha) < p^n \quad \text{in case } \mathbf{(2b)} \\ & (|C| = p^n). \end{cases}$$

We then set

$$V_s = \prod_{\alpha} V_{\alpha,s} \tag{7.27}$$

noting that these are finite products in view of s having finite support. We make the important observation that for each $\alpha = (\lambda_i, \Delta_j, g_k)$ involved in V_s the F-deg of $\lambda_i^{\Delta_j g_k}$ in V_s is precisely $s(\alpha)$. Conversely we have

Lemma 7.6.1 *Let M be given by (7.23) and $h_{ijk} = h(\alpha)$ be the F-deg of $\lambda_i^{\Delta_j g_k}$ in M for each $\alpha = (\lambda_i, \Delta_j, g_k)$. Then $M \equiv V_s\,(mod\, I_2(C))$ where $s(\alpha) = h(\alpha)$ for all α.*

Proof. In cases **(1a)** and **(1b)** there is nothing to prove. Case **(2a)** is a consequence of repeated applications of the observation that, given $m = p + q$ (thus $q < m$)

$$\left(\lambda^{g\theta^l}\right)^m \equiv \left(\lambda^{g\theta^l}\right)^p \left(\lambda^{g\theta^l}\right)^q \equiv \left(\lambda^{g\theta^{l+1}}\right) \left(\lambda^{g\theta^l}\right)^q.$$

If $|C| = p^n < \infty$, then $\lambda^{p^n} - \lambda \in I_2(C)$ and $\lambda^{\theta^l} - \lambda^{p^l} \in I_2(C)$. Hence case **(2b)** follows from repeated application of the following fact that, given $m = p^n + k$ (thus $m \equiv k + 1\,(mod\, p^n - 1)$)

$$\lambda^m \equiv \lambda^{p^n} \lambda^k \equiv \lambda^{k+1}.$$

Theorem 7.6.2 *The V_s's (as defined in (7.27)) are a C-basis for $C[\Lambda^{T_0}]$ modulo $I_2(C)$.*

Proof. In cases **(1a)** and **(1b)** the result is clear since $I_2(C) = 0$ and the V_s's coincide with the monomials given in (7.23).

In case **(2a)** the fact that the V_s's are a C-spanning set modulo $I_2(C)$ is given by Lemma 7.6.1. To show that the V_s's are C-independent modulo $I_2(C)$ we define a C-linear transformation $\chi : C[\Lambda^{T_0}] \to C[\Lambda^{T_0}]$ as follows. For each monomial M in (7.23) we map M to that V_s in (7.27) such that for each λ^{g_k} the F-deg of λ^{g_k} in M is the same as F-deg of λ^{g_k} in V_s. Clearly χ acts as the identity on each V_s. On the other hand consider an element of the form

$$M\left[\left(\lambda^{g\theta^l}\right)^p - \lambda^{g\theta^{l+1}}\right] = M\left(\lambda^{g\theta^l}\right)^p - M\lambda^{g\theta^{l+1}} \qquad (7.28)$$

where M is as in (7.23). Evidently the F-deg of $\lambda_i^{g_k}$ in each summand of (7.28) is the same and so χ maps (7.28) to 0, whence χ maps $I_2(C)$ to 0. If $\sum c_s V_s \in I_2(C)$ then

$$0 = \chi\left(\sum c_s V_s\right) = \sum c_s \chi(V_s)$$

and so $c_s =$ for all s.

In case **(2b)** we conclude from Lemma 7.6.1 that the V_s's are a C-spanning set of $C[\Lambda^{T_0}]$ modulo $I_2(C)$. Next we consider the C-linear transformation χ of $C[\Lambda^{T_0}]$ defined as in the case **(2a)**. For any element of the form

$$M\left[\lambda^{\theta^l} - \lambda^{p^l}\right] = M\lambda^{\theta^l} - M\lambda^{p^l} \tag{7.29}$$

where M is as in (7.23), the F-deg of λ_i in each summand of (7.29) is the same and so χ maps (7.29) to 0. Hence χ maps $I_2(C)$ to 0. Since χ acts as the identity on each V_s, we infer that the V_s's are linearly independent modulo $I_2(C)$. The theorem is thereby proved.

The C-span of the V_s's in Theorem 7.6.2 will be denoted by $P(C)$ and the elements of $P(C)$ will be called *F-reduced* . Clearly we have the C-space decomposition

$$C[\Lambda^{T_0}] = I_2(C) \oplus P(C)$$

where $I_2(C)$ is the set of F-trivial T-identities of C. Thus our stated goal of showing that any T-identity of C is F-trivial is equivalent to showing any F-reduced T-identity of C is 0.

The analysis of case **(1b)** will prove to the most complicated and we first require a digression into the theory of algebraically dependent homomorphisms of a field into itself (the need for this is brought about by the fact that in case **(1b)** the map $c \mapsto c^p$ is a homomorphism but not an automorphism).

Let C be a field, and let $C[\Lambda]$ be the free commutative algebra in Λ over C. We note that $C[\Lambda]$ is a subalgebra of $C[\Lambda^{T_0}]$ and we may on occasion use this inclusion to connect results in $C[\Lambda]$ with our usual general setting. For example if C is a finite field of order p^m a polynomial $\phi(\lambda_1, \lambda_2, \ldots, \lambda_n) \in C[\Lambda]$ is commonly called "reduced" if $\deg_{\lambda_i}(\phi) < p^m$ for each i or, equivalently, ϕ is an F-reduced element of $C[\Lambda^{T_0}]$. We begin with the well-known

Remark 7.6.3 *Let $\phi = \phi(\lambda_1, \lambda_2, \ldots, \lambda_n) \in C[\Lambda]$ (and assumed to be "reduced" if C is finite) such that $\phi(c_1, c_2, \ldots, c_n) = 0$ for all $c_1, c_2, \ldots, c_n \in C$. Then $\phi = 0$.*

A polynomial $\phi(\lambda_1, \lambda_2, \ldots, \lambda_n)$ is said to be *additive* if

$$\phi(\lambda_1 + \mu_1, \ldots, \lambda_n + \mu_n) = \phi(\lambda_1, \ldots, \lambda_n) + \phi(\mu_1, \ldots, \mu_n),$$

where $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n$ are distinct indeterminates in Λ. Next let A be an additive abelian group and let $h_1, h_2, \ldots, h_n$ be additive mappings of A into the additive group of C (we are primarily interested in the case when $A = C$). Then $h_1, h_2, \ldots, h_n$ are said to be *algebraically dependent via* ϕ over C if $0 \neq \phi(\lambda_1, \lambda_2, \ldots, \lambda_n) \in C[\Lambda]$ is such that

$$\phi(a^{h_1}, a^{h_2}, \ldots, a^{h_n}) = 0 \quad \text{for all} \quad a \in A.$$

Theorem 7.6.4 (Artin) *If $h_1, h_2, \ldots, h_n : A \to C$ are algebraically dependent via $\phi(\lambda_1, \lambda_2, \ldots, \lambda_n)$ over C then there exists a nonzero additive polynomial $\psi(\lambda_1, \lambda_2, \ldots, \lambda_n)$ such that*

$$\psi(a^{h_1}, a^{h_2}, \ldots, a^{h_n}) = 0 \quad \textit{for all} \quad a \in A$$

and $\deg_{\lambda_i}(\psi) \leq \deg_{\lambda_i}(\phi)$ *for each i.*

Proof. For convenience we shall write $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$, $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$, $\widehat{a} = (a^{h_1}, a^{h_2}, \ldots, a^{h_n})$, $\vec{a} = (a_1, a_2, \ldots, a_n)$. Let $\psi(\lambda)$ be a nonzero polynomial of smallest total degree $\deg_\lambda \psi$ for which $\deg_{\lambda_i}(\psi) \leq \deg_{\lambda_i}(\phi)$ for each i and for which $\psi(\widehat{a}) = 0$ for all $a \in A$. We claim that $\psi(\lambda)$ is the desired polynomial.

Indeed, suppose to the contrary that ψ is not additive. Choosing new variables $\mu_1, \mu_2, \ldots, \mu_n$ we are thus assuming that

$$\chi(\lambda, \mu) = \psi(\lambda + \mu) - \psi(\lambda) - \psi(\mu) \neq 0.$$

It is easy to see that

$$\deg(\chi) \leq \deg(\psi), \ deg_{\lambda_i}(\chi) \leq \deg_{\lambda_i}(\psi), \ \deg_{\mu_i}(\chi) \leq \deg_{\lambda_i}(\psi),$$

and $\chi(\widehat{a}, \widehat{b}) = 0$ for all $a, b \in A$. Suppose first that $\chi(\vec{c}, \widehat{b}) = 0$ for all $c_1, c_2, \ldots, c_{\in}C^n$, $b \in A$. By Remark 7.6.3 we may pick $\vec{c}, \vec{d} \in C^n$ such that $\chi(\vec{c}, \vec{d}) \neq 0$, since $\chi \neq 0$. Setting $\sigma(\mu) = \psi(\vec{c}, \mu)$ we note that $\sigma(\mu) \neq 0$, $\sigma(\widehat{b}) = 0$ for all $b \in A$,

$$\deg(\sigma) \leq \deg_(\ \mu)(\chi) < \deg(\phi), \ \deg_{\mu_i}(\sigma) \leq \deg_{\mu_i}(\psi),$$

and thus we have a contradiction to the choice of ψ. Therefore we may suppose there exist $\vec{c} \in C^n$, $b \in A$ such that $\chi(\vec{c}, \widehat{b}) \neq 0$. Setting $\tau(\lambda) = \chi(\lambda, \widehat{b})$, we see that $\tau(\lambda) \neq 0$, $\tau(\widehat{a}) = 0$ for all $a \in A$,

$$\deg(\tau) \leq \deg_(\ \lambda)(\chi) < \deg(\phi), \ \deg_{\lambda_i}(\tau) \leq \deg_{\lambda_i}(\psi),$$

and again we have a contradiction to the choice of ψ.

We next characterize additive polynomials.

Theorem 7.6.5 *A polynomial $\phi = \phi(\lambda_1, \lambda_2, \ldots, \lambda_n) \in C[\Lambda]$ is additive if and only if it has the form $\sum a_i \lambda_i$ (char$(C) = 0$) or $\sum_{i=1}^n \sum_{j \geq 0} a_{ij} \lambda_i^{p^j}$ (char$(C) = p$).*

Proof. Clearly the indicated polynomials are additive. Conversely, setting $\phi_i(\lambda_i) = \phi(0, \ldots, 0, \lambda_i, 0, \ldots, 0)$, we see by the additivity of ϕ that $\phi(\lambda_1, \lambda_2, \ldots, \lambda_n) = \sum_{i=1}^n \phi_i(\lambda_i)$, and so we may assume without loss of generality that $\phi = \sum a_j \lambda^j$ is a polynomial in one variable. It is immediate from additivity that $a_0 = 0$. Suppose that $a_r \neq 0$ for some $r > 0$. From

$\phi(\lambda+\mu)-\phi(\lambda)-\phi(\mu)=0$ (μ a new indeterminate) it follows that $a_r\left[(\lambda+\mu)^r-\lambda^r-\mu^r\right]=0$ and in particular $ra_r\lambda^{r-1}\mu=0$. If $char(C)=0$ then we have the immediate contradiction $a_r=0$ and we are done. If $char(C)=p$, then p divides r and we may write $r=sp^k$, $k\geq 1$ and $(p,\, s)=1$. Then

$$\begin{aligned} 0 &= (\lambda+\mu)^r-\lambda^r-\mu^r=(\lambda+\mu)^{p^ks}-\lambda^{p^ks}-\mu^{p^ks} \\ &= \left(\lambda^{p^k}+\mu^{p^k}\right)^s-(\lambda^{p^k})^s-(\mu^{p^k})^s. \end{aligned}$$

If $s>1$ it follows that $s\left(\lambda^{p^k}\right)^{s-1}\mu^{p^k}=0$, a contradiction since $(p,\, s)=1$. Therefore $r=p^k$ and the proof of the theorem is complete.

Functions $h_1,h_2,\ldots,h_n$ of a set S into C are said to be *linearly dependent* over C if there exists $0\neq\sum_{i=1}^n c_i\lambda_i$ such that $\sum_{i=1}^n c_is^{h_i}=0$ for all $s\in S$. A useful condition for linear independence is given in

Theorem 7.6.6 (Artin) *If $h_1,\ldots,h_n$ are distinct homomorphisms of a group G into the multiplicative group of C, then they are linearly independent over C.*

Proof. Suppose $h_1,h_2,\ldots,h_n$ are linearly dependent. By suitable reordering we may assume that $h_1,h_2,\ldots,h_m$ is a minimal dependent subset of $\{h_1,\ldots,h_n\}$, satisfying, say, $\sum_{i=1}^m c_i\lambda_i$. Clearly $m>1$. We pick $a\in G$ such that $a^{h_1}\neq a^{h_2}$, and let $g\in G$. On the one hand $0=\sum c_i(ag)^{h_i}=\sum c_ia^{h_i}g^{h_i}$ whereas on the other hand $0=a^{h_1}\sum c_ig^{h_i}=\sum c_ia^{h_1}g^{h_i}$. Subtracting second equation from the first yields $\sum_{i=2}^m c_i\left(a^{h_i}-a^{h_1}\right)g^{h_i}=0$ contradicting the minimality of m since $c_2\left(a^{h_2}-a^{h_1}\right)\neq 0$.

Our digression is now complete and we return to the task of showing that F-reduced T-identities of C are 0.

Lemma 7.6.7 *Fix $\lambda\in\Lambda$ and let ϕ be an F-reduced T-identity of C involving only λ. Then $\phi=0$.*

Proof. We suppose $\phi \neq 0$ and write ϕ in the standard form

$$\sum_s c_s V_s, \quad V_s = \prod_\alpha V_{\alpha,s}, \quad \alpha_1 = \lambda$$

according to (7.27). In case **(2b)** (C finite) $\phi = 0$ by Remark 7.6.3 since ϕ is a reduced polynomial in λ. In case **(1a)** we choose new indeterminates λ_α for each α involved in ϕ (finite in number), set $h_\alpha = \Delta_j g_k \in End_\Phi(C)$, set

$$\sigma = \sum_s c_s \left(\prod_\alpha \lambda_\alpha^{s(\alpha)}\right),$$

and note that the h_α's are algebraically dependent via σ (here $\alpha = (\lambda,\, \Delta_j,\, g_k)$). In case **(2a)** for each $(\alpha,\, l)$ involved in ϕ (finite in number) we choose a new indeterminate $\lambda_{\alpha,l}$, set $h_{\alpha,l} = g_k\theta^l \in End_\Phi(C)$, set

$$\sigma = \sum_s c_s \left(\prod_{\alpha,l} \lambda_{\alpha,s}^{s_l(\alpha)}\right),$$

and note that the $h_{\alpha,l}$'s are algebraically dependent via σ. By Theorem 7.6.4 and Theorem 7.6.5 the h_α's are linearly dependent over C and also the $h_{\alpha,l}$'s are linearly dependent over C (since in case **(2a)** we have $s_l(\alpha) < p$). Translated back to our usual setting, this simply says that there exists a nonzero reduced linear T-identity in λ satisfied by C. This is contradictory to Theorem 7.5.6 and so the proof is complete in cases **(1a)**, **(2a)** and **(2b)**.

For the remainder of the proof we assume case **(1b)** and write in detail

$$\phi = \sum_s c_s \prod_{j,k} \left(\lambda^{\Delta_j g_k}\right)^{s_{jk}}.$$

This in turn may be further explicitly written as

$$\phi = \sum_s c_s \prod_{j,k,l} \left[\left(\lambda^{\Delta_j g_k}\right)^{p^l}\right]^{s_{jkl}}, \ 0 \leq s_{jkl} < p,$$

where $s_{jk} = \sum_{l\geq 0} s_{jkl}p^l$. Setting $\beta = (j, k, l)$ we let $\{\lambda_\beta\}$ be distinct indeterminates in Λ, and for each β let h_β denote that additive map $\Delta_j g_k \sigma_l$, where σ_l stands for the homomorphism $c \mapsto c^{p^l}$. Now set $\psi = \sum_s c_s \prod_\beta \lambda_\beta^{s_\beta}$, where $s_\beta = s_{jkl} < p$ and note that $\psi(c^{h_\beta}) = 0$ for all $c \in C$, i.e., the maps h_β are algebraically dependent. By Theorem 7.6.4 and Theorem 7.6.5 there is a nonzero linear element $\sum_\beta c_\beta \lambda_\beta$ (since $s_\beta < p$) such that

$$\chi = \sum_\beta c_\beta \left(\lambda^{\Delta_j g_k}\right)^{p^l}$$

is a nonzero T-identity on C. We choose $\mu \neq \lambda \in \Lambda$ and make the substitution $\lambda \mapsto \lambda\mu^p$ in χ. From $(\mu^p)^\delta = p\mu^{p-1}\mu^\delta = 0$ it is clear that $(\mu^p)^{\Delta_j} = 0$, whence we see that

$$\chi(\lambda\mu^p) = \sum_\beta c_\beta \left[(\lambda\mu^p)^{\Delta_j g_k}\right]^{p^l} = \sum_\beta c_\beta \left(\lambda^{\Delta_j g_k}\right)^{p^l} (\mu^{g_k})^{p^{l+1}}.$$

$\chi(\lambda\mu^p)$ of course remains a T-identity on C and so, recalling the notation $\sigma_l : c \mapsto c^{p^l}$, we have

$$\sum_\beta c_\beta \left(c^{\Delta_j g_k}\right)^{p^l} r^{g_k \sigma_{l+1}} = 0 \quad \text{for all} \quad c, r \in C.$$

We claim that the homomorphisms $\{g_k \sigma_{l+1}\}$ are distinct. Indeed, suppose $g_{k_1}\sigma_{l_1+1} = g_{k_2}\sigma_{l_2+1}$, with $l_1 \geq l_2$. Then $\sigma_{l_1+1} = g_{k_1}^{-1} g_{k_2} \sigma_{l_2+1}$, i.e.,

$$c^{p^{l_1+1}} = \left(c^{g_{k_1}^{-1} g_{k_2}}\right)^{p^{l_2+1}}$$

whence $c^{p^m} = c^{g_{k_1}^{-1} g_{k_2}}$, $m = l_1 - l_2 \geq 0$. Thus $g_{k_1}^{-1} g_{k_2} \in G_f = 1$ and so $k_1 = k_2$ and accordingly $l_1 = l_2$. Therefore by Theorem 7.6.6 we see that for each k, l $\sum_j c_j \left(c^{\Delta_j g_k}\right)^{p^l} = 0$ for all $c \in C$, where $c_j = c_\beta$, $\beta = (j, k, l)$, i.e.,

$$\sum_j c_j \left(\lambda^{\Delta_j g_k}\right)^{p^l} \tag{7.30}$$

is a nonzero T-identity. Applying g_k^{-1} to (7.30) we see that

$$\sum_j c_j^{g_k^{-1}} \left(\lambda^{\Delta_j}\right)^{p^l} \tag{7.31}$$

is a nonzero T-identity. Now we let $L = \{c^{p^l} \mid c \in C\}$, choose an L-basis $\{v_i\}$ of C, and write $c_j^{g_k^{-1}} = \sum_i c_{ij}^{p^l} v_i$. Then, substituting $\lambda \mapsto c$ in (7.31), we have

$$\sum_i \left(\sum_j c_{ij}^{p^l} \left(c^{\Delta_j}\right)^{p^l} \right) v_i = 0,$$

whence for each i $\sum_j c_{ij}^{p^l} \left(c^{\Delta_j}\right)^{p^l} = 0$, and hence $\sum_j c_{ij} c^{\Delta_j} = 0$. Thus $\sum_j c_{ij} \lambda^{\Delta_j} = 0$ is a nonzero linear T-identity, a contradiction to Theorem 7.5.6, and the proof of the lemma is complete.

We are ready to show that for a field C the only T-identities are F-trivial.

Theorem 7.6.8 *If ϕ is an F-reduced T-identity on a field C, then $\phi = 0$. In other words, every T-identity is F-trivial.*

Proof. We suppose $\phi \neq 0$. Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the indeterminates involved in ϕ. We proceed by induction on n. The case $n = 1$ is given by Lemma 7.6.7. We may write ϕ in the form $\phi = \sum_{s_1} \Psi_{s_1} V_{s_1}$, where $V_{s_1} = \prod_{\alpha_1 = \lambda_1} V_{\alpha,s}$ and Ψ_{s_1} is an F-reduced element in $\lambda_2, \lambda_3, \ldots, \lambda_n$. Taking into account the induction assumption, we conclude that it is enough to prove that Ψ_{s_1} is a T-identity of C. If not there is a T-substitution $\lambda_i \mapsto r_i$, $r_i \in C$, $i = 2, 3, \ldots, n$ such that for some s_1 $\Psi_{s_1}(r_2, r_3, \ldots, r_n) \neq 0$. We set $c_{s_1} = \Psi_{s_1}(r_2, r_3, \ldots, r_n)$ and note that $\sum c_{s_1} \Psi_{s_1}$ is a nonzero F-reduced T-identity of C, a contradiction to Lemma 7.6.7. Thus $\Psi_{s_1} = 0$ and so $\phi = \sum_{s_1} \Psi_{s_1} V_{s_1} = 0$, a contradiction. The proof of the theorem is thereby complete.

We close this section with the following well-known criteria of linear independence of functions and its corollary.

Lemma 7.6.9 *Functions $h_1, h_2, \dots, h_n$ of a set S into C are linearly independent if and only if there exist $a_1, a_2, \dots, a_n \in S$ such that* $\det(h_i(a_j)) \neq 0$.

Proof. The "if" part is almost immediate. Indeed, suppose $\sum_{i=1}^n c_i h_i = 0$, $c_i \in C$. Since $\det(h_i(a_j)) \neq 0$, the n equations $\sum_{i=1}^n c_i h_i(a_j) = 0$, $j = 1, 2, \dots, n$ have only the trivial solution for the c_i's.

Suppose that $h_1, h_2, \dots, h_n$ are linearly independent. We proceed by induction on n. The case $n = 1$ is obvious. For the $n \times n$ matrix $A = (h_i(a_j))$ we denote by A_{ij} the i, j-cofactor. By the induction assumption there exist $a_1, a_2, \dots, a_{n-1} \in S$ such that $A_{n,n} = \det(h_i(a_j))_{i,j=1}^{n-1} \neq 0$. Suppose that $\det(h_i(a_j))_{i,j=1}^{n} = 0$ for all $a_n \in S$. Then expanding we obtain $\sum_{i=1}^n A_{i,n} h_i(a_n) = 0$ and so $\sum_{i=1}^n A_{i,n} h_i(t) = 0$ in $t \in S$ which means that $h_1, \dots, h_n$ are linearly dependent, a contradiction.

Corollary 7.6.10 *Let $\phi_1, \phi_2, \dots, \phi_m$ be F-reduced elements of $C[\Lambda^{T_0}]$ involving the indeterminates $\lambda_1, \lambda_2, \dots, \lambda_m$. Then ϕ_i, $1 \leq i \leq m$, are C-independent if and only if there exist m substitutions $a^{(j)} = (a_{j1}, a_{j2}, \dots, a_{jm}) \in C^m$ such that* $\det(\phi_i(a^{(j)})) \neq 0$.

7.7 The Structure of T-identities (General Case)

One of the main results proved so far in this chapter (Theorem 7.5.8) states that if R is a prime ring and ϕ is a nonzero reduced T-identity on a nonzero ideal I of R, then R is GPI. This result will be used in the present section, in which our aim is to show that such a ϕ above enjoys two very strong properties:

(a) (very roughly stated) the variables involved in ϕ may be partially "freed";

(b) ϕ is a T-identity on $Q = Q_s(R)$.

We mention that if $\phi \in \mathcal{E}^*$ (reduced with no antiautomorphisms involved) and $char(R) = 0$ then nothing further need be said - Theorem 7.5.9 says that the variables may be completely "freed" and ϕ is a GPI on Q. Thus this section is of interest only if $char(R) = p$ or antiautomorphisms are involved.

Whereas the meaning of **(b)** is quite clear we need to extend the notion of Frobenius automorphism defined in the preceding section for fields to prime rings in order to clarify **(a)**. To this end let $g \in G = G(R)$, the group of automorphisms and antiautomorphisms of the prime ring R, and let $\widehat{g}$ be the restriction of g to C. We say that g is a *Frobenius element* if $\widehat{g}$ is a Frobenius automorphism of C (as defined in section 7.6), and we let G_f denote the set of all Frobenius elements of G. We leave it as a routine exercise for the reader to show that $G_i \subseteq G_f \subseteq G$. We now fix (for the remainder of this section) a set G_{0f} of representatives of G modulo G_f and a set G_{fi} of representatives of G_f modulo G_i. We may then set $G_0 = G_{0f}G_{fi}$ and therefore take $T_0 = T_0(R)$ to be the set

$$\{\Delta g f \mid \Delta \in \mathcal{W}_0,\ g \in G_{0f},\ f \in G_{fi}\}.$$

Given a C-basis $\mathcal{A}$ of Q we know that a typical C-basis monomial M in $Q_C{<}X^{T_0}{>}$ may now be written

$$M = a_0 x_{i_1}^{\Delta_{j_1} g_{k_1} f_{l_1}} a_1 \dots x_{i_n}^{\Delta_{j_n} g_{k_n} f_{l_n}} a_n \tag{7.32}$$

where

$$a_i \in \mathcal{A},\ x_{i_q} \in X,\ \Delta_{j_q} \in \mathcal{W}_0,\ g_{k_q} \in G_{0f},\ f_{l_q} \in G_{fi}.$$

An arbitrary $\phi \in Q_C{<}X^{T_0}{>}$ can thus be written

$$\phi = \sum c_M M,\ c_M \in C \tag{7.33}$$

where M is of the form (7.32). To remind us of the variables involved in ϕ we will sometimes write $\phi = \phi(x_i^{\Delta_j g_k f_l})$.

We are now in a position to accurately explain property **(a)** stated at the beginning of this section. Let $\{y_{ijk}\}$ be a set of distinct indeterminates of X in one-one correspondence with the variables $x^{\Delta_j g_k}$, and let $\phi = \phi(x_i^{\Delta_j g_k f_l})$ be a nonzero reduced T-identity on some nonzero ideal I of R. Then (**(a)**) may be restated as

(a)′ $\phi(y_{ijk}^{f_l})$ is a T-identity on some nonzero ideal J of R.

If we wish to focus on a particular x in the monomial M in (7.32) it is convenient to rewrite (7.32) as

$$M = P_0 x^{\Delta_{j_1} g_{k_1} f_{l_1}} P_1 \dots P_{n-1} x^{\Delta_{j_n} g_{k_n} f_{l_n}} P_n \tag{7.34}$$

where $P_0, P_1, \dots, P_n$ are monomials of the form (7.32) not involving x. In turn if we wish to concentrate on a particular triple x, Δ, g in (7.34) we shall write

$$M = Q_0 x^{\Delta g f_1} Q_1 \dots Q_{n-1} x^{\Delta g f_n} Q_n \tag{7.35}$$

where $Q_0, Q_1, \dots, Q_n$ are monomials of the form (7.32) whose variables are not $x^{\Delta g f_l}$ for any l.

At this point we make an observation relating $T_0(R)$ and $T_0(C)$ which will be used in the sequel.

Remark 7.7.1 *If R is GPI then $T_0(C)$ may be chosen so that*
(i) $\mathcal{W}_0(R) \subseteq \mathcal{W}_0(C)$ and
(ii) $G_{0f}(R) \subseteq G_{0f}(C)$.

Proof. Since R is a GPI we know by Theorem 4.5.3 that if $\delta \in D(R)$ is such that δ vanishes on C, i.e. $\widehat{\delta} = 0$, then $\delta \in D_i(R)$. In this situation we then conclude that a basis $\mathcal{B}_0(C)$ of $Der(C)$ may be chosen so that $\mathcal{B}_0(R)$ maps injectively into $\mathcal{B}_0(C)$. It follows (from the PBW Theorem) that $\mathcal{W}_0(R)$ maps injectively into $\mathcal{W}_0(C)$, thus proving **(i)**. The proof of **(ii)** follows easily from the definition of Frobenius elements.

Now assume that R is GPI and consider the extended setting

$$\mathcal{S}_1(R) = \mathcal{S}_0(C) \otimes_C \mathcal{S}(R)$$

together with the C-ring map $\gamma : T(R) \to End_\Phi(\mathcal{S}_1(R))$ given by Remark 7.3.6. Given $x, y \in X$, $\lambda \in \Lambda$ we now make the T-substitution $x \mapsto x + \lambda y$ of $\mathcal{S}(R)$ into $\mathcal{S}_1(R)$ relatively to γ (Here, to simplify the notation, we are writing $x+\lambda y$ for $1 \otimes x + \lambda \otimes y$). For any $\Delta_j = \delta_1 \delta_2 \ldots \delta_q \in \mathcal{W}_0(R)$, $g_k \in G_{0f}$, $f_l \in G_{fi}$, we may use the Leibnitz formulas to obtain

$$(x + \lambda y)^{\widetilde{\Delta_j} \widetilde{g_k} \widetilde{f_l}} = \sum_{\Delta'_j} \lambda^{\Delta'_j g_k \widehat{f_l}} y^{\Delta''_j g_k f_l} \tag{7.36}$$

where the summation is as described in Remark 1.1.1 and

$$\begin{gathered} \Delta_j, \Delta'_j, \Delta''_j \in \mathcal{W}_0(R) \subseteq \mathcal{W}_0(C), \quad g_k \in G_{0f}(R) \subseteq G_{0f}(C), \\ \widetilde{\Delta_j} = \gamma(\Delta_j), \quad \widetilde{g_k} = \gamma(g_k), \quad \widetilde{f_l} = \gamma(f_l). \end{gathered}$$

Notice that the slight abuse of notation in (7.36) is justified in view of our tacit use of Remark 7.7.1. However we definitely want to distinguish between $f_l \in G_{fi}$ and $\widehat{f_l} \in G_f(C)$, e.g. it might well be the case that the $\widehat{f_l}$ are all equal to 1.

Next let $\{V_s\}$ be the C-basis of $C{<}\Lambda^{T_0(C)}{>}$ modulo $I_2(C)$ as given by (7.27) and Theorem 7.6.2. We fix a nonzero ideal I of R. Then any $\psi \in \mathcal{S}_1$ can be written uniquely as

$$\psi = \sum_s V_s \otimes \phi_s + \chi \tag{7.37}$$

where $\phi_s \in Q_C{<}X^{T_0(R)}{>}$ and $\chi \in \mathcal{S}_1$ is sent to 0 (in view of Remark 7.3.7) by every C-algebra map $\lambda_j \mapsto c_j \in C$ $(\lambda_j \in \Lambda)$, $x_i \mapsto r_i \in J$ $(x_i \in X)$, with $c_j J \subseteq I$ (for a given ψ only a finite number of λ_i's are involved). For future reference we shall call ϕ_s the coefficient of V_s in (7.37).

Given $x \in X$, $\Delta \in \mathcal{W}_0$, $g \in G_{0f}$ we proceed to define the notion of the *Frobenius degree* (briefly, F-deg) of $x^{\Delta g}$ in any element ϕ of $Q_C{<}X^{T_0(R)}{>}$. We begin by defining for each $f \in G_{fi}$ according to the cases **(1a)**, **(1b)**,**(2a)** and **(2b)** described in section 7.6:

$$|f| = \begin{cases} 1 & \text{in cases } \mathbf{(1a)} \text{ and } \mathbf{(1b)} \\ p^l & \text{if } \quad \widehat{f} = \theta^l \quad \text{in cases } \mathbf{(2a)} \text{ and } \mathbf{(2b)}. \end{cases}$$

Here we recall that $\widehat{f}$ (the restriction of f to C) is a Frobenius automorphism of C by the definition of G_{0f}. Note that in case **(2a)** $|f|$ is not an integer if $l < 0$, whereas in case **(2b)** $|f|$ is an integer since $0 \leq l < m$ where $|C| = p^m$. We also remark that in view of Theorem 4.5.3 $D(R) = D_i(R)$ (and so $\mathcal{W}_0 = 1$) in cases **(2a)** and **(2b)** since $Der(C) = 0$ as was shown in section 7.6.

Regarding a monomial M as written in the form (7.35) we then define the F-deg of $x^{\Delta g}$ in M to be equal to

$$\begin{array}{ll} 0 \quad \text{if} \quad x^{\Delta g} \quad \text{does not appear in} \quad M, & \\ \sum_{l=1}^{n} |f_l| = n \quad \text{in cases } \mathbf{(1a)} \text{ and } \mathbf{(1b)}, & \\ \sum_{l=1}^{n} |f_l| \quad \text{in case } \mathbf{(2a)}, & (7.38) \\ r \quad \text{in case } \mathbf{(2b)}, \text{ where} \qquad \sum_{l=1}^{n} |f_l| - 1 = q(p^n - 1) + r_0, & \\ \quad 0 \leq r_0 < p^n - 1, \ r = r_0 + 1. & \end{array}$$

We remark that in cases **(1a)** and **(1b)** the F-deg of $x^{\Delta g}$ in M is just the ordinary degree of the variable $x^{\Delta g}$ in M. In case **(2a)** we note that the F-deg of x^g (since $\Delta = 1$) in M need not be an integer (if $l < 0$). For $\phi \in Q_C{<}X^{T_0}{>}$ we write $\phi = \sum c_M M$ as in (7.33) and define the F-deg of $x^{\Delta g}$ in ϕ to be the maximal F-deg of $x^{\Delta g}$ in all M's belonging to ϕ.

For induction purposes later on the following partially ordered set will be useful. For fixed $x \in X$, $g \in G_{0f}$ any variable of the form $x^{\Delta_j g f_l}$ will be called an *(x, g)-variable* . If

$\phi \in Q_C < X^{T_0} >$, i.e., ϕ is reduced, the largest Δ_j appearing in any (x, g)-variable belonging to ϕ will be denoted by $\overline{\Delta} = \overline{\Delta}(\phi; x; g)$. (In case no (x, g)-variable belongs to ϕ we have $\overline{\Delta} = 1$). If m is a fixed integer, possibly negative, we define $S = S(m; x; g)$ to be the set of all reduced elements ϕ whose (x, g)-variables $x^{\Delta_j g f_l}$ are such that $|f_l| \geq p^m$. We partially order S as follows

(i) First compare $\overline{\Delta}(\phi; x; g)$,

(ii) If **(i)** is inconclusive, then compare the F-deg of $x^{\overline{\Delta} g}$ in ϕ. We note that for any $\phi \in S$ the F-deg of $x^{\overline{\Delta} g}$ in ϕ lies in the set N_m of all rational numbers $\{\sum_{l \geq m} a_l p^l \mid a_l \geq 0\}$. Since both $\mathcal{W}_0$ and N_m are well ordered sets it follows that S satisfies the minimum condition under the partial ordering just described. We set $N_{-\infty} = \cup_{m \in Z} N_m$.

We now come to a rather technical lemma in which in a special instance of (7.35) we are able to compute the coefficient of one of the V_s's. This will be of crucial importance when we come to establishing property **(a)**.

Lemma 7.7.2 *Assume C is infinite and R is GPI, fix $x, y \in X$, $\lambda \in \Lambda$, $g \in G_{0f}(R)$, $h \in N_{-\infty}$, and let $M \in Q_C<T_0(R)>$ be a monomial of the form*

$$M = Q_0 x^{\overline{\Delta} g f_1} Q_1 \dots Q_{n-1} x^{\overline{\Delta} g f_n} Q_n \tag{7.39}$$

where (as in (7.35)) the Q_i's do not involve any variable of the form $x^{\overline{\Delta} g f}$ for any f and $\overline{\Delta} = \overline{\Delta}(M; x; g)$. Let $M(x + \lambda y)$ be the element of $\mathcal{S}_1$ obtained from M by replacing x by $x + \lambda y$ and leaving x_i, $x_i \neq x$, alone, and let V be the C-basis monomial in $C[\Lambda^{T_0(C)}]$ given by $V = V_{\alpha,s} = V_s$, where $\alpha = (\lambda, \overline{\Delta}, g)$ is the sole support of s and $s(\alpha) = h$. Then the coefficient M_V of V in the expansion of $M(x + \lambda y)$ in $\mathcal{S}_1$ is nonzero if and only if $h = \sum_{l=1}^n |f_l|$, in which case

$$M_V = Q_0(x) y^{g f_1} Q_1(x) \dots Q_{n-1}(x) y^{g f_n} Q_n(x).$$

Proof. As a first step we consider any variable $x^{\Delta_j g_k f_l}$ appearing in M, look at the expansion of $(x+\lambda y)^{\widetilde{\Delta_j}\widetilde{g_k}\widetilde{f_l}}$ in (7.36), and ask under what circumstances does

$$\lambda^{\Delta'_j g_k \widehat{f_l}} = \lambda^{\overline{\Delta} g \theta^q} \quad \text{for some} \quad q.$$

Necessarily $g_k = g$ and $\Delta'_j = \overline{\Delta}$. But $\Delta'_j \leq \Delta_j$ and by the maximality of $\overline{\Delta}$ we then have $\Delta_j = \overline{\Delta}$. Since all of the variables involved in the Q_i's in (7.39) are distinct from $x^{\overline{\Delta} g f_l}$, it follows by completely expanding $(x+\lambda y)$ by means of (7.36) that the one and only one summand in this expansion containing V as a factor is

$$\begin{aligned} & Q_0(x)\lambda^{\overline{\Delta} g \widehat{f_1}} y^{g f_1} Q_1(x) \ldots Q_{n-1}(x)\lambda^{\overline{\Delta} g \widehat{f_n}} y^{g f_n} Q_n(x) \\ = & \left(\prod_{l=1}^{n} \lambda^{\overline{\Delta} g \widehat{f_l}}\right) \otimes Q_0(x) y^{g f_1} Q_1(x) \ldots Q_{n-1}(x) y^{g f_n} Q_n(x) \end{aligned}$$

subject to the condition

$$V \equiv \prod_{l=1}^{n} \lambda^{\overline{\Delta} g \widehat{f_l}} \,(mod\, I_2(C)). \tag{7.40}$$

But (7.40) is equivalent to $\sum_{l=1}^{n} |f_l| = h$, and the lemma is proved.

The preceding lemma will be used in proving the following lemma, which in turn goes a long way towards establishing property **(a)**.

Lemma 7.7.3 *Let C be infinite and let ϕ be a reduced T-identity on a nonzero ideal I of R. For fixed $x \in X$, $g \in G_{0f}$, $\overline{\Delta} = \overline{\Delta}(\phi;\, x;\, g)$, and $y \in X$ not appearing in ϕ, let τ be the element obtained from ϕ by substituting y^g in place of $x^{\overline{\Delta} g}$ but leaving all other variables $x_i^{\Delta_j g_k f_l}$ intact. Then τ is a reduced T-identity on some nonzero ideal J of R.*

Proof. We may suppose $\phi \neq 0$ and hence by Theorem 7.5.8 that R is GPI. Suppose to the contrary that τ is not a reduced identity on any $0 \neq J \lhd R$ and choose $m \in \mathcal{Z}$ such that for every $(x,\ g)$-variable $x^{\Delta_j g f_l}$ belonging to ϕ we have $|f_l| \geq p^m$ (If $G_f = 1$ we take $m = 0$). The subset S_0 of $S(m;\ x;\ g)$ consisting of all reduced T-identities ϕ_0 on some nonzero ideal of R which are no longer T-identities on some nonzero ideal of R when $x^{\overline{\Delta}_0 g}$ is replaced by y^g, $\overline{\Delta}_0 = \overline{\Delta}(\phi_0;\ x;\ g)$, is therefore nonempty. Hence S_0 has a minimal member which, without loss of generality, we shall again designate as ϕ (and assume is a T-identity on I). We set $h = F$-deg of $x^{\overline{\Delta} g}$ in ϕ, $\overline{\Delta} = \overline{\Delta}(\phi;\ x;\ g)$ and write

$$\phi = \sum c_M M, \quad c_M \in C$$

where (with (7.33) in mind) M is of the form

$$M = Q_0 x^{\overline{\Delta} g f_1} Q_1 \ldots Q_{n-1} x^{\overline{\Delta} g f_n} Q_n$$

where in turn the Q_l's are monomials whose variables are distinct from $x^{\overline{\Delta} g f_l}$. In

$$\mathcal{S}_1(R) = C[\Lambda^{T_0(C)}] \otimes_C Q_C{<}X^{T_0(R)}{>}$$

we form the element $\phi(x + \lambda y)$, $\lambda \in \Lambda$, $y \in X$ distinct from all indeterminates in ϕ, by replacing any variable $x^{\Delta_j g_k f_l}$ by $(x + \lambda y)^{\widetilde{\Delta_j}\widetilde{g_k}\widetilde{f_l}}$ as expanded in (7.36) but leaving all variables x_i, $x_i \neq x$ alone. We may then write

$$\phi(x + \lambda y) = \sum_{s \in K} V_s(\lambda) \otimes \phi_s(x, x_1, x_2, \ldots, x_q, y) + \chi$$

according to (7.37), where $w = |K| < \infty$. By Corollary 7.6.10 there exists elements $c_t \in C$, $t \in K$, such that the $w \times w$ matrix $(V_s(c_t))_{s,t \in K}$ is nonsingular. We may choose a nonzero ideal $J \subseteq I$ such that $c_t J \subseteq I$ for $t \in K$. Hence $\phi(x + \lambda y)$ vanishes under any substitution in which λ is mapped to c_t and x, x_i, y are mapped arbitrarily into J. Now consider the w equations

$$\sum_{s\in K} V_s(c_t)\phi_s(r, r_1, \dots, r_q, a) = 0, \quad t \in K$$

formed by sending

$$\lambda \mapsto c_t, \ x \mapsto r, \ x_i \mapsto r_i, \ y \mapsto a, \ r, r_i, a \in J.$$

Since $(V_s(c_t))$ is nonsingular, each $\phi_s(r, r_1, \dots, r_q, a) = 0$, i.e., each $\phi_s(x, x_1, \dots, x_q, y)$ is a T-identity on J.

In particular let $V = V_{\alpha,s} = V_s$, where $\alpha = (\lambda, \overline{\Delta}, g)$ is the sole support of s and $s(\alpha) = h$ (here we recall that h is the F-deg of $x^{\overline{\Delta}g}$ in ϕ). We have just shown that the coefficient of $\phi_V = \phi_s$ of V in the expansion of $\phi(x + \lambda y)$ in $\mathcal{S}_1$ is also a T-identity on some nonzero ideal $J \subseteq I$ of R. We now proceed to determine ϕ_V. Let

$$M = Q_0 x^{\overline{\Delta}gf_1} Q_1 \dots Q_{n-1} x^{\overline{\Delta}gf_n} Q_n,$$

written in the form (7.35), be any one of the monomials in (7.37) belonging to ϕ. By Lemma 7.7.2 the coefficient M_V of V in the expansion of $M(x + \lambda y)$ is nonzero if and only if the F-deg of $x^{\overline{\Delta}g}$ in M is equal to h (the F-deg of $x^{\overline{\Delta}g}$ in ϕ), in which case

$$M_V = Q_0(x) y^{gf_1} Q_1(x) \dots Q_{n-1}(x) y^{gf_n} Q_n(x).$$

Therefore

$$\phi_V = \sum \{c_M M_V \mid F\text{-deg of } x^{\overline{\Delta}g} \text{ in } M \text{ is equal to } h\}$$

and M_V is obtained from M by replacing $x^{\overline{\Delta}gf_l}$ by y^{gf_l}, $l = 1, 2, \dots, n$. Now let ϕ' be the element of $Q_C{<}X^{T_0}{>}$ obtained from ϕ_V by substituting $x^{\overline{\Delta}}$ for y, i.e.

$$\phi' = \sum \{c_M M \mid F\text{-deg of } x^{\overline{\Delta}g} \text{ in } M \text{ is equal to } h\}$$

There exists a nonzero ideal $K \subseteq J$ such that $K^{\overline{\Delta}} \subseteq J$(e.g., take $K = J^r$, where $r = |\overline{\Delta}|+1$). Since ϕ_V is a T-identity on J it follows that ϕ' is a T-identity on K. Clearly $\phi' \in S = S(m, x, g)$, but $\phi' \notin S_0$. Consider the element $\psi = \phi - \phi'$. Certainly $\psi \neq 0$, since otherwise we would have the contradiction $\phi \notin S_0$. From the definition of ϕ' it is clear that $\overline{\Delta}(\psi;\, x;\, g) \leq \overline{\Delta}(\phi;\, x;\, g)$, and that the F-deg of $x^{\overline{\Delta}g}$ in ψ is strictly less than h (the F-deg of $x^{\overline{\Delta}g}$ in ϕ). Therefore $\psi < \phi$ (in the ordering in S) and so by the minimality of ϕ in S_0 we conclude that $\psi \notin S_0$, i.e. substitution of $x^{\overline{\Delta}g}$ by y^g in ψ produced a T-identity ρ on some nonzero ideal $L \subseteq K$. The element $\phi_V + \rho$ is then the required element, and the proof of the lemma is complete.

We are now in a position to establish property **(a)**$'$.

Theorem 7.7.4 *Let R be a prime ring, let $\phi(x_i^{\Delta_j g_k f_l})$ be a reduced T-identity on a nonzero ideal I of R, and let $\{y_{ijk}\}$ be distinct elements of X in one-one correspondence with the variables $x_i^{\Delta_j g_k}$. Then $\phi(y_{ijk}^{f_l})$ is a T-identity on some nonzero ideal J of R.*

Proof. If $\phi = 0$ there is nothing to prove, and so we may assume that $\phi \neq 0$. Then by Theorem 7.5.8 R is GPI and so by Remark 7.7.1 $\mathcal{W}_0(R) \subseteq \mathcal{W}_0(C) = \mathcal{W}(C)$ and $G_{0f}(R) \subseteq G_{0f}(C)$.

Suppose C is finite. Then $Der(C) = 0$ and $G_{0f}(C) = 1$, whence $\mathcal{W}_0(R) = 1$ and $G_{0f}(R) = 1$. Therefore in this case $\phi = \phi(x_i^{f_l})$ is already of the required form.

We may therefore assume that C is infinite. For fixed $x \in X$, $g \in G_{0f}$ let

$$\overline{\Delta}(\phi;\, x;\, g) = \Delta_1 > \Delta_2 > \ldots > \Delta_t$$

be the $\Delta_j \in \mathcal{W}_0(R)$ involved in the $(x,\, g)$-variables of ϕ. Let ψ_1 be the element obtained from ϕ by by substituting z_1^g in place of $x^{\Delta_1 g}$ (and leaving all other variables intact) where z_1 is a new indeterminate. By Lemma 7.7.3 ψ_1 is a T-identity on some nonzero ideal $I_1 \subseteq I$. Since $\Delta_2 = \overline{\Delta}(\psi_1; x; g) < \Delta_1$ we see again by Lemma 7.7.3 that ψ_2, the element obtained from ψ_1 by replacing $x^{\Delta_2 g}$ by z_2^g, is a T-identity on some nonzero ideal $I_2 \subseteq I_1 \subseteq I$. Continuing in this fashion, after t steps we have shown that by substituting z_j^g for $x^{\Delta_j g}$ in ϕ, $j = 1, 2, \ldots, t$, the element $\psi = \psi_{x,g}$ so obtained is a T-identity on some nonzero ideal J of R. Substituting now $y_i^{g^{-1}}$ for z_i, $i = 1, 2, \ldots, t$ (and leaving all other variables intact) where $y_1, y_2, \ldots, y_t$ are new variables, we obtain the element $\tau = \tau_{x,g}$ which is a T-identity on $U = J \cap J^g$. We note that the element τ is obtained from ϕ by replacing $x^{\Delta_j g}$ by y_j. Now let

$$(x, g) = (x_{i_1}, g_{i_1}), (x_{i_2}, g_{i_2}), \ldots, (x_{i_n}, g_{i_n})$$

be the (necessarily finite) subset of $X \times G_{0f}$ such that ϕ has (x_{i_j}, g_{i_j})-variables. Repeated application of the preceding argument then completes the proof of the theorem.

We now turn our attention to verifying property **(b)**. In view of Theorem 7.7.4 we shall assume for the remainder of this section that any T-identity ϕ is of the form $\phi = \phi(x_i^{f_l})$. As an initial goal our aim will be to show that any T-identity on $0 \neq I \lhd R$ is a T-identity on the socle of RC. To do this we first need some further definitions. We shall say that ϕ is additive on an additive subgroup A of Q if for each $x_i \in X$ involved in ϕ we have

$$\phi(r_i + s_i) = \phi(r_i) + \phi(s_i) \quad \text{for all} \quad r_i, s_i \in A.$$

Next recall the definition of N:

$$N = \begin{cases} \mathcal{N} & \text{if} \quad G_f(C) = 1 \\ \mathcal{N}_p & \text{if} \quad G_f(C) \neq 1,\ |C| = \infty. \end{cases}$$

Now let x be an indeterminate involved in ϕ (where ϕ is as shown in (7.33)) and let $h \in N$. The $\binom{x}{h}$-homogeneous part of

ϕ is defined to be

$$\begin{aligned}\mu_h \quad = \quad & \textstyle\sum\{c_M M \mid M \text{ belongs to } \phi \text{ and} \\ & \qquad F\text{-deg of } x \text{ in } M \text{ equals } h\}.\end{aligned}$$

Clearly, for fixed x, ϕ is uniquely representable as a sum of its $\binom{x}{h}$-homogeneous parts:

$$\phi = \sum \mu_h.$$

Likewise if $x_1, x_2, \ldots, x_m$ are all the indeterminates involved in ϕ and $h_1, h_2, \ldots, h_m \in N$, then the $\binom{x_1, x_2, \ldots, x_m}{h_1, h_2, \ldots, h_m}$-homogeneous part of ϕ (which will sometimes be referred to as an F-homogeneous part of ϕ) is defined to be

$$\mu = \sum\{c_M M \mid F\text{-deg of } x_i \text{ in } M \text{ equals } h_i,\ 1 \leq i \leq m\}.$$

As above ϕ can be written as the direct sum of its F-homogeneous parts.

Lemma 7.7.5 *Let C be infinite. Then $\phi(x_i^{f_l})$ is a T-identity on a nonzero ideal of R if and only if each F-homogeneous component of ϕ is a T-identity on a nonzero ideal of R.*

Proof. The "if" part being obvious, we assume ϕ is a T-identity on I and fix any one of the indeterminates involved in ϕ. Let $h_1, h_2, \ldots, h_n$ be the distinct F-deg's of x in the various monomials belonging to ϕ. We write $\phi = \sum_{i=1}^{n} \tau_i$ where $\tau_i = \mu_{h_i}$ is the $\binom{x}{h_i}$-homogeneous part of ϕ. In the extended setting

$$\mathcal{S}_1 = \mathcal{S}_1(R) = S_0(C) \otimes_C \mathcal{S}(R)$$

we choose $\lambda \in \Lambda$ and consider the element $\phi(\lambda x)$ obtained from ϕ by substituting λx for x and leaving x_i, $x_i \neq x$, alone. From

$$(\lambda x)^{\gamma(f)} = \lambda^{\widehat{f}} x^f$$

(where γ is given by Remark 7.3.6) it is easy to see that $\tau_i(\lambda x) = M_i(\lambda)\tau_i(x) + \chi_i$ (as in (7.37)), where $M_i(\lambda)$ is one of the basis monomials (7.23) in which the F-deg of λ is h_i. By Lemma 7.6.1

$$M_i(\lambda) \equiv V_{s_i}(\lambda)\,(mod\, I_2(C)).$$

Therefore

$$\phi(\lambda x) = \sum_{i=1}^{n} V_{s_i}(\lambda)\tau_i(x) + \chi,$$

noting that $V_{s_1}, V_{s_2}, \ldots, V_{s_n}$ are C-independent modulo $I_2(C)$. By Corollary 7.6.10 there exist $c_1, c_2, \ldots, c_n \in C$ such that the $n \times n$ matrix $(V_{s_i}(c_j))$ is invertible. Let $0 \neq J \lhd R$ be such that $J \subseteq I$ and $Jc_j \subseteq I$, $j = 1, 2, \ldots, n$, and note that the following n equations hold:

$$0 = \phi(c_j r) = \sum_{i=1}^{n} V_{s_i}(c_j)\tau_i(r), \quad j = 1, 2, \ldots, n$$

for all $r \in J$ and $r_k \in J$, $x_k \neq x$. From the invertibility of $(V_{s_i}(c_j))$ we conclude that $\tau_i(r) = 0$ for all $r, r_k \in J$, i.e., $\tau_i = \mu_{h_i}$ is a T-identity on J for $i = 1, 2, \ldots, n$. Repetition of the above process applied to each μ_{h_i} and using indeterminates involved in ϕ other than x clearly leads ultimately to each F-homogeneous part of ϕ being a T-identity on some nonzero ideal of R.

Lemma 7.7.6 *Let C be infinite and let $\phi = \phi(x_1, x_2, \ldots, x_n)$ be a T-identity on $0 \neq I \lhd R$, $\binom{x_1, x_2, \ldots, x_n}{h_1, h_2, \ldots, h_n}$-homogeneous, and additive on IC. Then ϕ is a T-identity on IC.*

Proof. In $\mathcal{S}_1 = \mathcal{S}_0(C) \otimes_C \mathcal{S}(R)$ we select indeterminates $\lambda_1, \lambda_2, \ldots, \lambda_n \in \Lambda$ and, using the homogeneity of ϕ and Theorem 7.6.2 we observe that

$$\phi(\lambda_1 x_1, \lambda_2 x_2, \ldots, \lambda_n x_n) = V\phi(x_1, x_2, \ldots, x_n) + \chi$$

where V is that basis monomial in (7.27) whose F-deg in each λ_i is h_i. It follows that

$$\phi(c_1r_1, \ldots, c_nr_n) = V(c_1, \ldots, c_n)\phi(r_1, \ldots, r_n) = 0 \qquad (7.41)$$

for all $c_i \in C$, $r_i \in I$. We now compute, using (7.41) and the additivity of ϕ on IC,

$$\begin{aligned}
&\phi(\sum c_{1j_1}r_{1j_1}, \sum c_{2j_2}r_{2j_2}, \ldots, \sum c_{nj_n}r_{nj_n}) \\
&= \sum_{j_1,j_2,\ldots,j_n} \phi(c_{1j_1}r_{1j_1}, c_{2j_2}r_{2j_2}, \ldots, c_{nj_n}r_{nj_n}) \\
&= \sum_{j_1,j_2,\ldots,j_n} V(c_{1j_1}, c_{2j_2}, \ldots, c_{nj_n})\phi(r_{1j_1}, r_{2j_2}, \ldots, r_{nj_n}) = 0
\end{aligned}$$

where $c_{ij_i} \in C$ and $r_{ij_i} \in I$.

Lemma 7.7.7 *If $\phi(x_i^{f_l})$ is a T-identity on $0 \neq I \triangleleft R$, then $\phi(x_i^{f_l})$ is a T-identity on JC for some $0 \neq J \triangleleft R$.*

Proof. If C is finite we can pick $0 \neq K \triangleleft R$ such that $KC \subseteq R$. Setting $J = IK$ we have

$$JC = I(KC) \subseteq IR \subseteq I$$

and the lemma is proved.

We may therefore assume that C is infinite. The proof is by induction on $ht(\phi)$. Suppose first that $ht(\phi) = 0$. Writing $\phi = \sum \mu$ as the sum of its F-homogeneous parts we know that each μ is of height 0 and consequently each μ is additive. Furthermore, by Lemma 7.7.5, there is a nonzero ideal J of R such that each μ is a T-identity on J. Lemma 7.7.6 then says that each μ, and hence ϕ, is a T-identity on JC and the lemma is proved in this case.

Now suppose the lemma is true for all ϕ of height less than n satisfying the conditions of the lemma. Let ϕ of height n satisfy the conditions of the lemma. Without loss of generality, in view of Lemma 7.7.5, we may assume that ϕ is F-homogeneous. This implies in particular that any x that appears in ϕ must appear in each monomial M involved in ϕ. Now let x be such an x, select a new indeterminate y, and form the element $M(x+y)-M(x)-M(y)$. If $\deg_x(M)=1$ then $M(x+y)-M(x)-M(y)=0$. If $\deg_x(M)>1$ then $ht(M(x+y)-M(x)-M(y))<ht(M)$. From these considerations it follows that for any x appearing in ϕ either $\phi(x+y)-\phi(x)-\phi(y)=0$ (if $\deg_x(\phi)=1$) or (if $\deg_x(\phi)>1$) $ht(\phi(x+y)-\phi(x)-\phi(y))<ht(\phi)$. Setting $\psi=\phi(x+y)-\phi(x)-\phi(y)$ we have that either $\psi=0$ (if $\deg_x(\phi)=1$) or (if $\deg_x(\phi)>1$) $ht(\psi)<ht(\phi)$. By induction the latter possibility implies that ψ is a T-identity on JC for some $0\neq J\lhd R$. In either case we see that ϕ is x-additive on JC. Since x was arbitrary it follows that ϕ is additive on KC for some $0\neq K\lhd R$, whence by Lemma 7.7.6 the proof is complete.

In view of Theorem 7.7.4 we are now in a position to establish property **(b)**.

Theorem 7.7.8 *Let R be a prime ring and let ϕ be a reduced T-identity on $0\neq I\lhd R$ of the form $\phi=\phi(x_i^{f_l})$. Then ϕ is a T-identity on $Q_s(R)$.*

Proof. We may assume $\phi\neq 0$, whence by Theorem 7.5.8 R is GPI. In this situation we know that RC is primitive with nonzero socle H, acting densely on a vector space V over a division ring D. By Theorem 4.3.8(**v**) $Q_s(RC)\subseteq End_D(V)$. Since $Q_s(R)\subseteq Q_s(RC)$ it suffices to show that ϕ is a T-identity on $Q_s(RC)$. By Lemma 7.7.7 ϕ is a T-identity on an ideal JC of RC for some $0\neq J\lhd R$ and so in particular ϕ is a T-identity on the socle H. Let $\mathcal{A}$ be a C-basis of $Q_s(R)$ and write

$$\phi=\sum c_M M,\quad c_M\in C,\quad \deg(\phi)=s$$

where M is a basis monomial of the form

$$M \quad = \quad a_{j_0}x_{i_1}^{f_{l_1}}a_{j_1}\dots a_{j_{n-1}}x_{i_n}^{f_{l_n}}a_{j_n}$$

$$x_i \in X, \quad a_j \in \mathcal{A}, \quad f_l \in G_{fi}.$$

Let $\mathcal{A}'$, X', G'_{fi} denote respectively the sets (necessarily finite) of all $a_j \in \mathcal{A}$, $x_i \in X$, $f_l \in G_{fi}$ appearing in ϕ. We may assume $X' = \{x_1, x_2, \ldots, x_m\}$ and we make an arbitrary but fixed substitution $x_i \mapsto q_i \in Q_s(RC)$, $i = 1, 2, \ldots, m$. Letting $v \in V$, our task is to show that $v\phi(q_1, q_2, \ldots, q_m) = 0$. To this end consider the D-span V_0 of all vectors $w \in V$ which are of one of the following two forms

$$\begin{aligned} w &= va_{j_0}q_{i_1}^{f_{l_1}}a_{j_1}\ldots a_{j_{r-1}}q_{i_r}^{f_{l_r}}a_{j_r} \quad \text{or} \\ w &= va_{j_0}q_{i_1}^{f_{l_1}}a_{j_1}\ldots a_{j_{r-1}}q_{i_r}^{f_{l_r}} \end{aligned} \tag{7.42}$$

where $0 \leq r \leq s$, $a_j \in \mathcal{A}'$, $f_l \in G'_{fi}$, $q_i \in \{q_1, q_2, \ldots, q_m\}$. V_0 is finite dimensional over D and therefore, since H acts densely on V, there exists $b \in H$ such that b is the identity on V_0. By Litoff's theorem there exists $e_0 \in H$ such that $b \in e_0He_0$. It follows that e_0 acts as the identity on V_0. Now consider the finite set $L = \{e_0^{f^{-1}} \mid f \in G'_{fi}\} \subseteq H$. Using Litoff's theorem again we know there is an idempotent $e \in H$ such that $L \subseteq eHe$. We claim that

$$e_0 = e_0e^f = e^fe_0, \quad f \in G'_{fi}.$$

Indeed, first assuming f is an automorphism, we have

$$e^fe_0 = \left(ee_0^{f^{-1}}\right)^f = \left(e_0^{f^{-1}}\right)^f = \left(e_0^{f^{-1}}e\right)^f = e_0e^f.$$

A similar argument prevails if f is an antiautomorphism. We next claim that if w is of the form (7.42) then $wq^f = w(eqe)^f$, $f \in G'_{if}$, $q \in \{q_1, q_2, \ldots, q_m\}$. Indeed,

$$\begin{aligned} w(eqe)^f &= we^fq^fe^f = we_0e^fq^fe^f = weq^fe^f = wq^fe^f \\ &= (wq^fe_0)e^f = (wq^f)ee^f = wq^fe = wq^f. \end{aligned}$$

From repeated use of this claim it follows that

$$\begin{aligned} &va_{j_0}q_{i_1}^{f_{l_1}}a_{j_1}\ldots a_{j_{n-1}}q_{i_n}^{f_{l_n}}a_{j_n} \\ &= va_{j_0}(eq_{i_1}e)^{f_{l_1}}a_{j_1}\ldots a_{j_{n-1}}(eq_{i_n}e)^{f_{l_n}}a_{j_n}. \end{aligned}$$

and thus

$$v\phi(q_1, q_2, ..., q_m) = v\phi(eq_1e, eq_2e, ..., eq_me) = 0$$

since $eq_ie \in H$, $i = 1, 2, \ldots, m$. This completes the proof of the theorem.

By combining Theorem 7.7.4 and Theorem 7.7.8 we have

Theorem 7.7.9 *Let R be a prime ring, let $\phi = \phi(x_i^{\Delta_j g_k f_l})$ be a reduced T-identity on some nonzero ideal of R, and let $\{y_{ijk}\}$ be distinct elements of X in one-one correspondence with variables $x_i^{\Delta_j g_k}$. Then $\phi(y_{ijk}^{f_l})$ is a T-identity on $Q_s(R)$.*

7.8 T-identities with Coefficients in Q_{mr}

This brief section is an appendix in which we indicate that, by making some natural alterations in the definitions but otherwise essentially keeping the same proofs, the main results on T-identities remain valid even when the coefficients are allowed to be in Q_{mr}. The main obstacle to overcome is the fact that whereas derivations and automorphisms of R can be lifted to Q_{mr} (Proposition 2.5.1 and Proposition 2.5.3) antiautomorphisms can in general only be lifted to Q_s (Proposition 2.5.4). This problem, however, is easily solved by modifying the definition of a T-substitution. All other obstacles have already been anticipated by results on Q_{mr} proved in Chapter 2, Chapter 4, and Chapter 6, and we shall indicate where these are used.

Let R be a prime ring with D, G, T, G^*, and T^* defined exactly as in sections 7.1 and 7.2. There are two obvious ways of generalizing the notion of the setting $\mathcal{S}$ of R. One is defined to be

$$\mathcal{S}_m = Q_{mr} \coprod_C C\{V \otimes_C T\}$$

which we shall call the *maximal setting* of R. The other is defined to be

$$\mathcal{S}_m^* = Q_{mr} \coprod_C C\{V \otimes_C T^*\}$$

which we shall call the $*$-*maximal setting* of R.

A substitution process compatible with $\mathcal{S}_m$ is, in general terms at first, described as follows. Let P be a C-algebra with 1 such that

(i) $P \supseteq Q_{mr}$;

(ii) $P \supseteq N$, N a C-subalgebra of P;

(iii) There is a C-ring map $\gamma : T \to End_\Phi(N)$.

Let $\psi : V \to N$ be any C-space map. Then (as in section 7.1) it is shown that there is a unique C-algebra map $\tilde{\psi} : \mathcal{S}_m \to P$ given by $q \mapsto q$, $q \in Q_{mr}$, and $v \otimes t \mapsto \psi(v)^{\gamma(t)}$. Such a map will be called the T'-substitution determined by ψ relative to γ. Fix any C-basis X of V. Now let $P = Q_{mr}$, $N = Q_s$, and $\gamma : T \to End_\Phi(Q_s)$ as given in section 7.1. Any nonzero ideal I of R is of course contained in Q_s and we shall say that an element ϕ of $\mathcal{S}_m$ is a T'-identity on I if ϕ is mapped to 0 under all T'-substitutions $\tilde{\psi}$ for which $\psi(X) \subseteq I$. As in sections 7.5 and 7.7 T'-substitutions of $\mathcal{S}_m$ into itself are needed, and here we take $P = \mathcal{S}_m$, $N = \mathcal{S}$, and $\gamma : T \to End_\Phi(\mathcal{S})$ as given by Theorem 7.3.5.

As for $\mathcal{S}_m^*$ let P be a C-algebra with 1 containing Q_{mr} and let $\gamma : T^* \to End_\Phi(P)$ be a fixed C-ring map. For any C-space map $\psi : V \to P$ the C-algebra map $\tilde{\psi} : \mathcal{S}_m^* \to P$ determined by $q \mapsto q$, $q \in Q_{mr}$, and $v \otimes t \mapsto \psi(v)^{\gamma(t)}$, $t \in T^*$, is called the T^*-*substitution* determined by ψ relative to γ. Now let $P = Q_{mr}$. Since derivations and automorphisms of R can be lifted to Q_{mr} (Propositions 2.5.1 and 2.5.3) it is clear that there are resulting maps $\alpha : U \to End_\Phi(Q_{mr})$ and $\beta : G^* \to End_\Phi(Q_{mr})$ which can be simultaneously extended to a C-ring map $\gamma : T^* \to End_\Phi(Q_{mr})$. We shall say that $\phi \in \mathcal{S}_m^*$ is a T^*-*identity on* $0 \neq I \lhd R$ if ϕ is mapped to 0 under all T^*-substitutions $\tilde{\psi}$ for which

$\psi(X) \subseteq I$. It is clear that the analogue of Theorem 7.3.5 is valid, namely, there is an appropriate C-ring map $\gamma : T^* \to End_\Phi(\mathcal{S}_m^*)$, and so we have the T^*-substitutions of $\mathcal{S}_m^*$ into itself which are needed for extending the results of sections 7.5 and 7.7.

By definition the set I_0' of all trivial T'-identities (resp. the set I_0^* of all trivial T^*-identities) is the ideal of $\mathcal{S}_m$ (resp., ideal of $\mathcal{S}_m^*$) generated by the same elements C_1', C_2' as were used to generate I_0. By definition the set of reduced elements of $\mathcal{S}_m$ relative to $(\mathcal{B}, <)$ (resp., reduced elements of $\mathcal{S}_m^*$) is the subring $\mathcal{E}_m = Q_{mrC} < X^{T_0} >$ (resp., $\mathcal{E}_m^* = Q_{mrC} < X^{T_0^*} >$). With no changes in the proof we have the decomposition theorem

Theorem 7.8.1 $\mathcal{S}_m = I_0' \oplus \mathcal{E}_m$ *and* $\mathcal{S}_m^* = I_0^* \oplus \mathcal{E}_m^*$.

We proceed to state the analogues of the main results proved in sections 7.5 and 7.7 (there are, of course, no problems with section 7.6), providing remarks at the key places where the coefficients of the identities are involved. We begin by stating the analogues of Theorem 7.5.5 (concerning linear T'-identities) and Theorem 7.5.6 (concerning linear T^*-identities).

Theorem 7.8.2 *Let* $0 \neq \phi \in Q_{mr}X^{T_0}Q_{mr}$ *be a* T'*-identity on some* $0 \neq I \triangleleft R$. *Then* R *is GPI.*

Theorem 7.8.3 *If* $\phi \in Q_{mr}X^{T_0^*}Q_{mr}$ *is a* T^**-identity on some* $0 \neq I \triangleleft R$, *then* $\phi = 0$.

Their proofs follow from the analogues of Lemmas 7.5.4, 7.5.3, 7.5.1, 7.5.2.

Concerning Lemma 7.5.4 the elements b_{ij}, $j = 1, 2, \ldots, m_i$, $i = 1, 2$ are only assumed to be in Q_{mr} rather than in Q_s. But Theorem 2.5.9 already anticipates this situation by providing $\beta = N_{I,J}$, I an ideal, J a dense right ideal, to be used instead of $\beta \in N_I$.

Concerning the analogue of the crucial Lemma 7.5.3 Remark 2.5.5 can be applied to the C-independent elements $b_1, \ldots, b_m$ in the reduction to equation (7.17). Next, for the finite collection b, v_i', w' in the equation (7.17), we must choose a dense right ideal J, with $J \subseteq I$, such that bJ, $v_i'J$, $w'J$ are all contained in R. Immediately following equation (7.18) we may use the ideal IbJ in the definition of f, noting that a typical element of IbJ can be expressed as $b \cdot \beta$, $\beta \in N_{I,J}$. Following equation (7.22) we need to know that $b_0 = b \cdot \gamma \in IbJ$. Indeed, since $Q_{mr}(J) = Q_{mr}(R)$ (Proposition 2.1.10), we may use Remark 2.5.5 (with J playing the role of R) to conclude that there exists $\gamma \in N_{I \cap J}$ such that $b_0 = b \cdot \gamma \in IbJ$, $b_0 \neq 0$, $b_j \cdot \gamma = 0$, $j = 2, 3, \ldots, m$. Finally, we need to make certain that the element u lies in Q_s. Having noted that $u \in Q_r$ we have $uK \subseteq R$ for some $0 \neq K \lhd R$. But there is an ideal $0 \neq L \lhd R$ such that $L^{\delta_1 + \sum \mu_i \alpha_i} \subseteq R$. From $\delta_1 + \sum \mu_i \alpha_i = ad(u)$, taking $P = K \cap L$, it is clear that $Pu \subseteq R$ whence $u \in Q_s$.

Concerning Lemma 7.5.1 we simply replace it by Corollary 6.3.16, and Lemma 7.5.2 may be replaced by Proposition 6.3.13.

With these remarks in place the proofs of Theorem 7.8.2 and Theorem 7.8.3 follow.

For the analogue of Theorem 7.5.8 the same proof by induction on deg(ϕ) goes through, the case $n = 1$ having been given by Theorem 7.8.2. We therefore may state

Theorem 7.8.4 *Let R be a prime ring and let $\phi \in \mathcal{E}_m$ be a nonzero reduced T'-identity on some nonzero ideal I of R. Then R is GPI.*

The analogue of the "freeness" theorem (Theorem 7.7.4) holds true without comment.

Theorem 7.8.5 *Let R be a prime ring, let $\phi(x_i^{\Delta_j g_k f_l}) \in \mathcal{E}_m$ be a reduced T'-identity on a nonzero ideal I of R, and let $\{y_{ijk}\}$ be distinct elements of X in one-one correspondence with the* *variables $x_i^{\Delta_j g_k}$. Then $\phi(y_{ijk}^{f_l})$ is a T'-identity on some nonzero ideal J of R.*

Finally, we remark that it is the "extension" theorem (Theorem 7.7.8) that really necessitated the creation of the two settings $\mathcal{S}_m$ and $\mathcal{S}_m^*$. For the setting $\mathcal{S}_m$ the analogue of Theorem 7.7.8 goes through with the same proof, since $x_i \mapsto q_i \in Q_s$ is the T'-substitution being used. For the setting $\mathcal{S}_m^*$ a slight adjustment must be made since the T^*-substitution $x_i \mapsto q_i \in Q_{mr}$ is required. The vector space V on which RC acts densely should be taken to be a right vector space V_Δ. Then by (the symmetric version of) Theorem 4.3.7(**viii**) we have $Q_{mr} \subseteq End(V_\Delta)$. Accordingly Q_{mr} acts on V from the left and the elements given in (7.42) should be appropriately rewritten to reflect this. We now state the two analogues of Theorem 7.7.8

Theorem 7.8.6 *Let R be a prime ring and let $\phi \in \mathcal{S}_m$ be a reduced T'-identity on $0 \neq I \triangleleft R$ of the form $\phi = \phi(x_i^{f_l})$, $f_l \in G_{fi}$. Then ϕ is a T'-identity on $Q_s(R)$.*

Theorem 7.8.7 *Let R be a prime ring and let $\phi \in \mathcal{S}_m^*$ be a reduced T^*-identity on $0 \neq I \triangleleft R$ of the form $\phi = \phi(x_i^{f_l})$, $f_l \in G_{fi} \cap G^*$. Then ϕ is a T^*-identity on $Q_{mr}(R)$.*

7.9 Applications

We present in this section several applications of the preceding results. Perhaps the most well-known is Kharchenko's characterization of algebraic derivations [146], and we begin with a generalization of this result (due to Leroy and Matczuk). Following this we present analogous results for algebraic automorphisms, and lastly we present some results on composition of derivations (due to Chebotar, Chuang and Lanski) which are generalizations of the well-known Posner's theorem on composition of two derivations of a prime ring.

Algebraic derivations. Let R be a prime ring with symmetric ring of quotients Q. We continue to use the various notations developed in earlier sections of this chapter. We shall also need on occasion to utilize the two-sided ring of right quotients $Q_r = Q_r(R) \supseteq Q$. Both C (acting on Q via right multiplications) and $D(R) = Der(R)C + D_i$ are subsets of $End_\Phi(Q)$ and in this framework we define the notion of an algebraic derivation.

Definition 7.9.1 *Let $\delta \in D(R)$, S a subring of Q, and $0 \neq I \triangleleft R$. Then δ is S-algebraic on I if*

$$\sum_{i=0}^{n} \delta^i a_i = 0 \quad \textit{(acting on } I\textit{)} \tag{7.43}$$

for some $n > 0$, $a_i \in S$, $a_n \neq 0$.

The condition (7.43) is equivalent to:

$$\sum_{i=0}^{n} x^{\delta^i} a_i \quad \text{is a } T\text{-identity on } I.$$

An application of Corollary 7.2.3(**ii**) and Theorem 7.5.6 yields

Remark 7.9.2 *$\sum_{i=0}^{n} \delta^i a_i = 0$ on I if and only if $\sum_{i=0}^{n} \delta^i a_i = 0$ on Q.*

In view of Remark 7.9.2 we may simply refer to δ as being S-algebraic (it is no longer necessary to add the phrase "on I"). If n is minimal in Definition 7.9.1 then n is called the S-deg of δ. Clearly, if δ is Q-algebraic, then δ is R-algebraic, with Q-deg of $\delta = R$-deg of δ. The question arises as to whether δ being Q-algebraic implies that δ is C-algebraic, and in the forthcoming characterization of algebraic derivations this question will be answered in the affirmative.

We look first at inner derivations.

Lemma 7.9.3 *Let $a \in Q$. Then the following are equivalent:*
(i) $ad(a)$ is C-algebraic;
(ii) $ad(a)$ is Q-algebraic;
(iii) a is C-algebraic.

Proof. Clearly **(i)** implies **(ii)**. If $ad(a)$ is Q-algebraic, then $\sum_{i=0}^{m}(l_a - r_a)^i a_i = 0$, $a_i \in Q$, $a_m \neq 0$, Since $Q_{(l)}Q_{(r)} \cong Q^\circ \otimes_C Q$ in view of Theorem 2.3.6, the above equation translates to $\sum_{i=0}^{m} a^i \otimes b_i = 0$ for suitable $b_i \in Q$, with $b_m = a_m \neq 0$. Choose a C-basis $v_1 = b_m, v_2, \dots, v_n$ of the vector space $\sum_{i=0}^{m} Cb_i$. Then we obtain that $\sum_{i=1}^{n} f_i(a) \otimes v_i = 0$ for suitable polynomials $f_i(x) \in C[x]$ and so $f_1(a) = 0$. Clearly $\deg(f_1(x)) = m$ and hence $f_1(x) \neq 0$. As a result a is C-algebraic and therefore **(ii)** implies **(iii)**. If a is C-algebraic, then the subring of $End_\Phi(Q)$ generated by l_a, r_a, and C is finite dimensional over C. Then $ad(a) = l_a - r_a$ is C-algebraic and so **(iii)** implies **(i)**.

We will also need the following

Remark 7.9.4 *Given $\delta \in D(R)$ and $0 \neq K \triangleleft R$ there exist nonzero ideals $K = L_0 \supseteq L_1 \supseteq L_2 \supseteq \dots$ such that $L_k^\delta \subseteq L_{k-1}$ for $k = 1, 2, 3, \dots$.*

Proof. Writing $\delta = \sum \delta_i c_i + \mu$, $\delta_i \in Der(R)$, $c_i \in C$, $\mu = ad(b)$, $b \in Q$, we may chose a nonzero ideal J of R such that $J + c_i J + bJ + Jb \subseteq K$. Setting $L_0 = K$ and $L_1 = J^3$ we see that $L_1^\delta \subseteq L_0$. Now we set $L_k = L_1^k$ and see by an easy induction on k that $L_k^\delta \subseteq L_{k-1}$.

We now proceed to prove a result of Leroy and Matczuk [187] which describes the nature of the equation of minimal degree satisfied by a Q-algebraic derivation.

Theorem 7.9.5 *Let $\delta \in D(R)$ be Q-algebraic of Q-*deg *n. Then there exist $q_0, q_1, \dots, q_n \in Q$, $q_n = 1$, such that:*
(i) $\sum_{i=0}^{n} \delta^i q_i = 0$, i.e., $\sum_{i=0}^{n} x^{\delta^i} q_i$ is a T-identity on Q;
(ii) $q_i^\delta = 0$ for all i, i.e., $[\delta, q_i] = 0$;
(iii) $[q_i, q_j] = 0$ for all i, j.

Proof. Without loss of generality we may assume that δ is R-algebraic of degree n. Let I be the subset of all $r \in R$ for which there exist $r_i \in R$, $i = 0, 1, \ldots, n-1$, such that

$$\delta^n r + \sum_{i=0}^{n-1} \delta^i r_i = 0 \tag{7.44}$$

The r_i's are uniquely determined by r (by the minimality of n), and it is clear that I is a nonzero right ideal of R. It follows from Remark 7.9.4 that there exists $0 \neq J \lhd R$ such that $J^{\delta^i} \subseteq R$ for all $i \leq n$. Now let $s \in Q$, $t \in J$, $r \in I$. From (7.44) we have

$$(st)^{\delta^n} r + \sum_{i=0}^{n-1} (st)^{\delta^i} r_i = 0 \tag{7.45}$$

Expansion of (7.45) by repeated use of the Leibnitz formulas results in

$$s^{\delta^n}(tr) + \sum_{i=0}^{n-1} s^{\delta^i} u_i = 0$$

where each u_i is of the form $\sum_{j=0}^{i} z_j t^{\delta j} r_{i+j}$, z_j an integer. Since $J^{\delta j} \subseteq R$ for each $j = 0, 1, \ldots, n$, we see that $u_i \in R$. We have thereby shown that $JI \subseteq I$. Now for each $i = 0, 1, \ldots, n-1$ we have a well-defined right R-module map $f_i : JI \to R$ given by $r \mapsto r_i$. Accordingly there exists $q_i \in Q_r$ such that $f(r) = r_i = q_i r$ for all $r \in JI$. Setting $q_n = 1$ we conclude that $(\sum_{i=0}^{n} \delta^i q_i)JI = 0$, whence

$$\sum_{i=0}^{n} \delta^i q_i = 0, \ q_i \in Q_r, \ q_n = 1.$$

We now claim that the q_i's lie in Q. Indeed, let $0 \neq K \lhd R$ such that $q_i K \subseteq R$ for all i. By Remark 7.9.4 there exist nonzero ideals $K = L_0 \supseteq L_0 \supseteq L_1 \supseteq \ldots \supseteq L_n$ such that $L_k^\delta \subseteq L_{k-1}$,

$k = 1, 2, \ldots, n$. Now let $s, t \in Q$. Making use of the Leibnitz formulas and the fact that $q_n = 1$ we have

$$0 = \sum_{i=0}^{n} (st)^{\delta^i} q_i - \sum_{i=0}^{n} s^{\delta^i} q_i t = \sum_{i=0}^{n-1} s^{\delta^i} u_i \tag{7.46}$$

where

$$u_i = \sum_{j=i+1}^{n} \binom{j}{i} t^{\delta^{j-i}} q_j + tq_i - q_i t = 0 \tag{7.47}$$

by the minimality of n. We now make the subclaim that $L_k q_{n-k} \subseteq R$ for $k = 0, 1, \ldots, n$, which we shall prove by induction on k. For $k = 0$ we have $L_0 q_n = K \subseteq R$. In the equation (7.47) we replace i by $n - k$ and set $l = j - (n - k)$. From the resulting equation we conclude that

$$L_k q_{n-k} \subseteq q_{n-k} L_k + \sum_{l=1}^{k} L_k^{\delta^l} q_{n-k+l} \tag{7.48}$$

By induction all summands on the right hand side of (7.48) lie in R and so the subclaim is proved. In particular $L_n q_i + q_i L_n \subseteq R$ for $i = 0, 1, \ldots, n$, i.e., each $q_i \in Q$, and so **(i)** is established.

An application of δ to $\sum_{i=0}^{n} s^{\delta^i} q_i = 0$, $s \in Q$, yields

$$\sum_{i=0}^{n} (s^\delta)^{\delta^i} q_i + \sum_{i=0}^{n-1} s^{\delta^i} q_i^\delta = 0.$$

Thus $\sum_{i=0}^{n-1} s^{\delta^i} q_i^\delta = 0$ and by the minimality of n we have $q_i^\delta = 0$ for each i and so **(ii)** is proved. Finally, making use of **(ii)** and the minimality of n, we see from

$$0 = \sum_{i=0}^{n} (sq_j)^{\delta^i} q_i - \sum_{i=0}^{n} s^{\delta^i} q_i q_j = \sum_{i=0}^{n-1} s^{\delta^i} [q_i, q_j]$$

that $[q_i, q_j] = 0$, thus establishing **(iii)**.

Proposition 7.9.6 *Let $\delta \in D(R)$ be Q-algebraic of Q-*deg n *and let $q_0, q_1, \ldots, q_n \in Q$ be given by Theorem 7.9.5. Suppose that $1 \cdot n \neq 0$ in Q. Then $\delta = ad(q_{n-1})/n$.*

Proof. We keep the notation of the proof of Theorem 7.9.5. Setting $i = n-1$ in (7.47), we obtain that $nt^\delta q_n + [t, q_{n-1}] = 0$ for all $t \in J$. Therefore $\delta - ad(-q_{n-1})/n$ vanishes on J. Since $Q = Q_s(J)$ and any derivation has a unique extension to Q, we see that $\delta = ad(-q_{n-1})/n$.

Theorem 7.9.7 *Let R be a prime ring of characteristic zero and let $\delta \in D(R)$. Then the following conditions are equivalent:*
(i) δ is C-algebraic;
(ii) δ is Q-algebraic;
(iii) $\delta = ad(a)$, $a \in Q$, a algebraic over C.

Proof. It is obvious that **(i)** implies **(ii)**. If δ is Q-algebraic, then $\delta = ad(a)$ for some $a \in Q$ by Proposition 7.9.6, because $1 \cdot n \neq 0$. Applying Lemma 7.9.3**(iii)**, we conclude that a is C-algebraic and so **(ii)** implies **(iii)**. The fact that **(iii)** implies **(i)** follows immediately from Lemma 7.9.3.

Theorem 7.9.8 *Let R be a prime ring of characteristic $p > 0$, and let $\delta \in D(R)$. Then the following conditions are equivalent:*
(i) δ is C-algebraic;
(ii) δ is Q-algebraic;
(iii) $\sum_{i=0}^m \delta^{p^i} c_i = ad(a)$ where $c_0, c_1, \ldots, c_m \in C$, $c_m \neq 0$, $a \in Q$, a algebraic over C.

Proof. The implication **(i)** implies **(ii)** is immediate. We now assume that **(ii)** holds. We know that $D(R)$ is a special restricted differential Lie algebra. Suppose first that $\delta_i = \delta^{p^i}$, $i = 0, 1, \ldots$, are right C-independent modulo D_i. Hence δ_i, $i = 0, 1, \ldots$, is a part of a well-ordered basis $\mathcal{B}_0$ of $D(R)$ modulo

D_i with $\delta_i < \delta_j$ in case $i < j$. Any positive integer i may be written uniquely in the form $\sum_{j=0}^{m_i} \alpha_{ij} p^j$, $0 \leq \alpha_{ij} < p$, and so $\delta^i = \prod_{j=0}^{m_i} \delta_j^{\alpha_{ij}}$ are part of a PBW-basis of $U(R)$ in view Theorem 5.4.5. This forces the contradiction to Theorem 7.5.6 that $\sum_{i=0}^{n} x^{\prod \delta_j^{\alpha_{ij}}} a_i \in Qx^{T_0^*}Q$ is a nonzero T-identity. We may thus conclude that $\mu = \sum_{i=0}^{m} \delta^{p^i} c_i = ad(a)$ for some choice of $c_i \in C$, $a \in Q$, $c_m \neq 0$. By Theorem 7.9.5

$$\sum_{i=0}^{n} \delta^i q_i = 0, \quad q_i \in Q, \; q_n = 1, \; [q_i, q_j] = 0, \; q_i^\delta = 0 \qquad (7.49)$$

where n is the Q-deg of δ. Let $S = C[q_0, q_1, \ldots, q_{n-1}]$ be the subring of $End_\Phi(Q)$ generated by C, $q_0, q_1, \ldots, q_{n-1}$ (regarded as right multiplications), and let M be the right S-submodule of $End_\Phi(Q)$ generated by $1, \delta, \delta^2, \ldots$. Since n is the Q-deg of δ, it follows from (7.49) that M is an n-generated free right module over the commutative ring S with the basis $1, \delta, \delta^2, \ldots, \delta^{n-1}$. Clearly $\delta \cdot M \subseteq M$ and so $\mu \cdot M \subseteq M$. Let $A \in M_n(S)$ be a matrix of the mapping $x \mapsto \mu \cdot x$, $x \in M$, and let $f(t) = |tE - A|$ be the characteristic polynomial of A. By Cayley-Hamilton theorem $f(\mu) \cdot x = 0$ for all $x \in M$. In particular $f(\mu) = f(\mu) \cdot 1 = 0$. Thus μ is Q-algebraic, and by Lemma 7.9.3 the element a is C-algebraic. Therefore **(ii)** implies **(iii)**.

Finally, assuming **(iii)**, we know that $ad(a)$ is C-algebraic by Lemma 7.9.3, and so we may write

$$\sum_{j=0}^{t} \left(\sum_{i=0}^{m} \delta^{p^i} c_i \right)^j d_j = 0, \quad c_i, d_j \in C, \; c_m \neq 0 \neq d_t \qquad (7.50)$$

Expansion of (7.50) using the commutation formula $c\delta = \delta c + c^\delta$ results in an equation

$$\delta^{tp^m} c_m d_t + \sum_{i=0}^{tp^m - 1} \delta^i c_i' = 0, \quad c_i' \in C$$

and so δ is C-algebraic, thus proving that **(iii)** implies **(i)**.

In closing we note that in 1957 Amitsur [1] proved the equivalence of **(i)** and **(iii)** in Theorem 7.9.7 in the case that R was a simple ring, the equivalence of **(i)** and **(iii)** in Theorem 7.9.7 and Theorem 7.9.8 was proved by Kharchenko [146] in 1978, and the additional equivalence with **(ii)** was proved by Leroy and Matczuk [187] in 1985.

Algebraic automorphisms. In this subsection we characterize algebraic automorphisms of prime rings in a somewhat analogous fashion to the results of preceding subsection. We refer the reader to the papers of Leroy and Matczuk [187], Page and Maoulaoui [199] from which these results are drawn.

Let R be a prime ring. The basic definitions we need are entirely analogous to those concerning derivations in the preceding subsection, and so we shall indicate these rather briefly. Let S be a subring of Q, and let $0 \neq I \triangleleft R$. An element $g \in Aut(R)$ is *S-algebraic on I* if $\sum_{i=0}^{n} g^i a_i = 0$ on I for some $n > 0$, $a_i \in S$, $a_n \neq 0$, or, equivalently, $\sum_{i=0}^{n} x^{g^i} a_i$ is a T-identity on I. As before, by Corollary 7.2.3 **(ii)** and Theorem 7.5.6, g is S-algebraic on I if and only if g is S-algebraic on Q (with the same equation in either case). The minimal such n is called the S-deg of g. We begin by characterizing X-inner automorphisms.

Theorem 7.9.9 *Let R be a prime ring and let $h = inn(s) \in G_i$ be an X-inner automorphism of R where $s \in Q$. Then the following conditions are equivalent:*

(i) h is C-algebraic;

(ii) h is Q-algebraic;

(iii) s is C-algebraic.

*If this situation holds, let l be the Q-*deg *of h, k the C-*deg *of h and m the C-*deg *of s. Then $l = m$, $k \leq l^2$, and $\sum_{j=0}^{l} h^j s^{l-j} c_j = 0$ for some $c_j \in C$, $c_l = 1$.*

Proof. In the course of showing the equivalence of **(i)**, **(ii)** and **(iii)** the second part of the theorem will be evident. The implication **(i)** implies **(ii)** being obvious, we assume $\sum_{j=0}^{l} h^j a_j =$

0, $a_j \in Q$, $a_l \neq 0$. This says that $\sum_{j=0}^{l} s^{-j}qs^j a_j = 0$ for all $q \in Q$, whence by Theorem 2.3.6 $\sum_{j=0}^{l} s^{-j} \otimes s^j a_j = 0$. Since $a_l \neq 0$ (and hence $s^l a_l \neq 0$) it follows that s^{-1} (and hence s) is C-algebraic of degree $m \leq l$ (thus establishing **(iii)**). Furthermore, writing $\sum_{j=0}^{m} s^{-j} c_j = 0$, $c_j \in C$, $c_m = 1$, we have

$$0 = \sum_{j=0}^{m} s^{-j} c_j q s^m = \sum_{j=0}^{m} s^{-j} q s^j (s^{m-j} c_j) = \sum_{j=0}^{m} q^{h^j} (s^{m-j} c_j)$$

for all $q \in Q$, i.e., $\sum_{j=0}^{m} h^j (s^{m-j} c_j) = 0$. From the minimality of l we conclude that $m = l$ and we have $\sum_{j=0}^{l} h^j (s^{l-j} c_j) = 0$.

Now assume that s is C-algebraic of degree m. Then l_s and r_s are algebraic elements of degree m in $End_{\Phi}(Q)$ and so the subring generated by l_s, r_s, and C in $End_{\Phi}(Q)$ is of dimension $\leq m^2$ over C, whence $h = inn(s) = l_{s^{-1}} r_s = l_s^{-1} r_s$ is C-algebraic of C-degree $k \leq m^2$. Having now shown **(i)** (and hence **(ii)**), we know that $m = l$ and so $k \leq l^2$. The proof is now complete.

Theorem 7.9.10 *Let R be a prime ring and let $g \in Aut(R)$. Then the following conditions are equivalent:*

(i) g is C-algebraic;

(ii) g is Q-algebraic;

(iii) For some positive integer v we have $g^v = inn(t)$ is X-inner, with t C-algebraic.

*If this situation holds, let m be the least positive integer for which $g^m = inn(s)$ is X-inner. Then s is C-algebraic (of, say, degree l), and if n is the Q-*deg *of g and k is the C-*deg *of g, then we have $n = ml$, $k \leq ml^2$, and $\sum_{j=0}^{l} g^{mj} s^{l-j} c_j = 0$ for some $c_j \in C$, $c_l = 1$.*

Proof. In the course of showing the equivalence of **(i)**, **(ii)**, **(iii)**, we shall at the same time be proving the rest of the theorem. Clearly **(i)** implies **(ii)**. Now assume g is Q-algebraic of degree n and write

$$\sum_{i=0}^{n} g^i a_i = 0, \quad a_i \in Q, \ a_n \neq 0 \tag{7.51}$$

Suppose first that for all $i \leq n$ g^i is not X-inner. Then $1, g, \ldots, g^n$ are distinct elements of $G_0(R)$ and

$$\sum_{i=0}^{n} x^{g^i} a_i \in Qx^{T_0^*}Q$$

is a T-identity on Q in contradiction to Theorem 7.5.6. Therefore $h = g^m = inn(s) \in G_i$ for some $0 < m \leq n$ and we may assume that m is minimal. Writing $n = ml + r$, $0 \leq r < m$ we rewrite (7.51) as

$$\sum_{i=0}^{r} g^i h^l a_{il} + \sum_{i=0}^{m-1} \sum_{j=0}^{l-1} g^i h^j a_{ij}, \quad a_{ij} \in Q, \ a_{rl} \neq 0,$$

in other words,

$$\sum_{i=0}^{r} s^{-l} x^{g^i} s^l a_{il} + \sum_{i=0}^{m-1} \sum_{j=0}^{l-1} s^{-j} x^{g^i} s^j a_{ij} \in Qx^{T_0^*}Q$$

is a reduced T-identity on Q. By Theorem 7.5.6 $\phi(x) = 0$ in $Qx^{T_0^*}Q$ and in particular for $i = r$ we have

$$s^{-l} x^{g^r} s^l a_{rl} + \sum_{j=0}^{l-1} s^{-j} x^{g^r} s^j a_{rj} = 0$$

that is,

$$0 = g^r h^l a_{rl} + \sum_{j=0}^{l-1} g^r h^j a_{rj} = g^r \left(\sum_{j=0}^{l} h^j a_{rj} \right)$$

and so

$$\sum_{j=0}^{l} g^{jm} a_{rj} = \sum_{j=0}^{l} h^j a_{rj} = 0, \quad a_{rl} \neq 0. \tag{7.52}$$

By the minimality of n we see that $r = 0$, and hence $n = ml$. Again by the minimality of n (7.52) says that h is Q-algebraic of degree l. By Theorem 7.9.9 we see that s is C-algebraic of degree l (thus proving **(iii)**), $\sum_{j=0}^{l} h^j s^{l-j} c_j = 0$ for some $c_j \in C$, $c_l = 1$, and the C-degree w of h satisfies $w \leq l^2$. It follows that $\sum_{j=0}^{l} g^{mj} s^{l-j} c_j = 0$ and $\sum_{i=0}^{w} g^{mi} d_i = 0$ for some $d_i \in C$, $d_w \neq 0$, whence the C-degree k of g satisfies the relation $k \leq ml^2$. Finally, suppose $f = g^v = inn(t)$ is X-inner with t C-algebraic. Let m be the least positive integer for which $h = g^m = inn(s)$ is X-inner. Writing $v = mq + r$, $0 \leq r < m$, we see from $f = h^q g^r$ that g^r is X-inner, whence $r = 0$ by the minimality of m. Thus $g^v = (g^m)^q$, leading to $inn(t) = inn(s^q)$, and so $s^q = tc$ for some $c \in C$. Therefore s is C-algebraic. By Theorem 7.9.9, h is C-algebraic and so g is C-algebraic, thus proving that **(iii)** implies **(i)**.

Products of derivations. In 1957 Posner proved that if R is a prime ring of characteristic distinct from 2 with nonzero derivations d_1 and d_2, then $d_1 d_2$ is not a derivation [241]. The question when a product of derivations is again a derivation was investigated by a number of authors, in particular by Krempa and Matczuk [153], by Chuang [84], by Lanski [168] and by Chebotar [78], some of whose results we shall present in this subsection. We begin with the following generalization of Martindale's lemma (i.e., Theorem 2.3.4) and a result of Bresar [68].

Lemma 7.9.11 *Let S be any set and R a prime ring with extended centroid C. Suppose that $F : S \to R$, $G : S \to R$ are nonzero mappings such that $F(s)xG(t) = \epsilon G(s)xF(t)$ for all $s, t \in S$, $x \in R$ and some fixed $0 \neq \epsilon \in C$. Then:*

(i) F and G are C-dependent;

(ii) $\epsilon = 1$.

Proof. Pick $t_0, s_0 \in S$ such that $F(t_0) \neq 0 \neq G(s_0)$. Then from $F(s_0)xG(t_0) = \epsilon G(s_0)xF(t_0)$ we conclude that $G(t_0) \neq 0$. Now from $F(s)xG(t_0) = \epsilon G(s)xF(t_0)$ we see that $F(s) = 0$ if and only if $G(s) = 0$. Suppose that $G(s) \neq 0$. Then $F(s)xG(t_0) - \epsilon G(s)xF(t_0)$ is a GPI on R and so by Corollary 6.1.3 we have that $G(t_0) = \lambda F(t_0)$ for some $\lambda \in C$. Hence

$$(\lambda F(s) - \epsilon G(s))xF(t_0) = 0 \quad \text{for all} \quad x \in R,\ s \in S.$$

Therefore $G = \epsilon^{-1}\lambda F$. Now we have

$$0 = F(t_0)xG(t_0) - \epsilon G(t_0)xF(t_0) = (\epsilon^{-1}\lambda - \lambda)F(t_0)xF(t_0)$$

for all $x \in R$. Thus $\epsilon = 1$ and the lemma is proved.

We continue with the following result of Posner [241].

Theorem 7.9.12 *Let R be a prime ring with extended centroid C and with nonzero derivations d_1, d_2 such that d_1d_2 is again a derivation of R. Then $char(R) = 2$ and there exists an element $c \in C$ such that $d_2 = d_1c$.*

Proof. Let $x, y \in R$. Then we have

$$(xy)^{d_1d_2} = x^{d_1d_2}y + x^{d_1}y^{d_2} + x^{d_2}y^{d_1} + xy^{d_1d_2} \tag{7.53}$$

On the other hand, since d_1d_2 is a derivation, we have

$$(xy)^{d_1d_2} = x^{d_1d_2}y + xy^{d_1d_2}$$

and so we conclude from (7.53) that

$$x^{d_1}y^{d_2} + x^{d_2}y^{d_1} = 0 \quad \text{for all} \quad x, y \in R \tag{7.54}$$

Substituting xz for x, we infer from (7.54) that

$$x^{d_1}zy^{d_2} + x^{d_2}zy^{d_1} = 0 \quad \text{for all} \quad x, y, z \in R \tag{7.55}$$

Hence by Lemma 7.9.11 $d_2 = d_2c$ for some $0 \neq c \in C$ and $-1 = 1$ which yields $char(R) = 2$.

Now we need the following general observation. Let R be a prime ring with extended centroid C and $D = D(R)$. Further let $\mathcal{B}_i$ be a linearly ordered C-basis of D_i and let $\mathcal{B}_0$ be a linearly ordered C-basis of D modulo D_i. As usual we assume that $\mathcal{B}_0 < \mathcal{B}_i$. Then $\mathcal{B}_0 \cup \mathcal{B}_i$ is a linearly ordered basis of D. Consider the corresponding PBW basis $\mathcal{W} = \mathcal{W}_0\mathcal{W}_i$ of the universal enveloping algebra U of the (restricted) differential C-Lie algebra D. Given $\Delta = \delta_1\delta_2\dots\delta_n \in \mathcal{W}_0$, where $\delta_i \in \mathcal{B}_0$ for all i, we set $|\Delta| = n$. Now let $x = \sum_{i=1}^m \Delta_i\Omega_i c_i$, where the $\Delta_i\Omega_i$'s are distinct elements of $\mathcal{W}$ and $0 \neq c_i \in C$. We set $|x| = \max\{|\Delta_i| \mid 1 \leq i \leq m\}$. Further given a natural number n, we denote by U_n the C-linear span of all products of the form $\Delta\Omega$, where $\Delta \in \mathcal{W}_0$ with $|\Delta| \leq n$ and $\Omega \in \mathcal{W}_i$. For ease with forthcoming formulas we also set $U_{-1} = \{0\}$.

Let $d_1, d_2, \dots, d_n \in D$. Suppose that $d_{s_1}, d_{s_2}, \dots, d_{s_m}$, where $1 \leq s_1 < s_2 < \dots < s_m \leq n$, forms a right C-basis of $\sum_{i=1}^n d_iC$ modulo D_i. Setting $\mu_j = d_{s_j}$ for $1 \leq j \leq m$, we shall assume that $\mu_1 < \mu_2 < \dots \mu_m \in \mathcal{B}_0$. Then we have that $d_i = \sum_{j=1}^m \mu_j c_{ij} + ad(a_i)$ for suitable $c_{ij} \in C$ and $ad(a_i) \in D_i$. Now consider the polynomial ring $A = C[x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n]$. Given a monomial $M = x_1^{k_1} \dots x_m^{k_m} y_1^{l_1} \dots y_n^{l_n}$ we set $\deg(M) = k_1 + k_2 + \dots + k_m$, $\deg_{x_i}(M) = k_i$, $\phi(M) = \mu_1^{k_1} \dots \mu_m^{k_m} ad(a_1)^{l_1} \dots ad(a_n)^{l_n}$ and extend ϕ to a right C-space map $\phi : A \to U$ by linearity. With reference to the observations and terminology just developed, the following lemma is due to Chebotar.

Lemma 7.9.13 *Let $i_1 < i_2 < \dots < i_k \leq n$ be those indices i such that $d_i = ad(a_i)$ (i.e., $c_{ij} = 0$ for all $j = 1, 2, \dots, m$). Suppose that either $char(R) = 0$, or $char(R) > n + 1 - k - m$. Set $f_i = \sum_{j=1}^m x_j c_{ij} + y_i$. Then:*

(i) $|d_1d_2 \dots d_n| = n - k$;

(ii) $d_1d_2 \dots d_n - \phi(f_1f_2 \dots f_n) \in U_{n-k-1}$.

Proof. Let $t_1, t_2, \ldots, t_m$ be nonnegative integers with $t_1 + t_2 + \ldots + t_m = r$, $1 \leq i \leq m$, $1 \leq s \leq k$ and $c \in C$. It follows from the formulas

$$\begin{aligned} c\mu_i &= \mu_i c + c^{\mu_i}, \\ ad(a)\mu_i &= \mu_i ad(a) + ad(a^{\mu_i}) \quad \text{and} \\ \mu_j\mu_i &= \mu_i\mu_j + [\mu_j, \, \mu_i] \end{aligned} \tag{7.56}$$

that

$$\begin{aligned} &\mu_1^{t_1} \ldots \mu_m^{t_m} ad(a_{i_1}) \ldots ad(a_{i_s}) c\mu_i \\ &-\mu_1^{t_1} \ldots \mu_{i-1}^{t_{i-1}} \mu_i^{t_i+1} \mu_{i+1}^{t_{i+1}} \ldots \mu_m^{t_m} ad(a_{i_1}) \ldots ad(a_{i_s}) c \\ &\in U_r \end{aligned} \tag{7.57}$$

We shall prove **(ii)** by induction on n. The case $n = 1$ is clear. Suppose now that our statement is proved for $d_1, d_2, \ldots, d_{n-1}$. Let $f_1 f_2 \ldots f_{n-1} = \sum_{j=1}^{t} M_t c_t$ where M_t's are distinct monomials and $0 \neq c_t \in C$. Consider the case $d_n = ad(a_n)$. Then among $d_1, d_2, \ldots, d_{n-1}$ there are exactly $k - 1$ X-inner derivations and so

$$\begin{aligned} &d_1 d_2 \ldots d_{n-1} - \phi(f_1 f_2 \ldots f_{n-1}) \\ &\in U_{(n-1)-(k-1)-1} = U_{n-k-1} \end{aligned} \tag{7.58}$$

Clearly

$$\phi(M_i) c_i ad(a_n) = \phi(M_i) ad(a_n) c_i = \phi(M_i y_n) c_i$$

and so $\phi(f_1 \ldots f_{n-1}) d_n = \phi(f_1 \ldots f_n)$. It follows from (7.58) that

$$\begin{aligned} d_1 \ldots d_n - \phi(f_1 \ldots f_n) &= (d_1 \ldots d_{n-1} - \phi(f_1 \ldots f_{n-1})) d_n \\ &\in U_{n-k-1} d_n \subseteq U_{n-k-1} \end{aligned}$$

and so in this case our statement is proved. Now suppose that $d_n \notin D_i$. Then we have

$$d_1 d_2 \ldots d_{n-1} - \phi(f_1 f_2 \ldots f_{n-1}) \in U_{n-k-2} \tag{7.59}$$

It follows from (7.57) that

$$\phi(f_1f_2\dots f_{n-1})\mu_i c_{ni} - \phi(f_1f_2\dots f_{n-1}x_ic_{ni}) \in U_{n-k-1}$$

and so

$$\phi(f_1f_2\dots f_{n-1})d_n - \phi(f_1f_2\dots f_n) \in U_{n-k-1}.$$

Now it is clear that

$$\begin{aligned} d_1\dots d_n - \phi(f_1\dots f_n) &= (d_1\dots d_{n-1} - \phi(f_1\dots f_{n-1}))d_n \\ &\quad +\phi(f_1f_2\dots f_{n-1})d_n - \phi(f_1f_2\dots f_n) \\ &\quad \in U_{n-k-2}d_n + U_{n-k-1} \subseteq U_{n-k-1} \end{aligned}$$

thus proving **(ii)**. Now let $f_1f_2\dots f_n = \sum_{l=1}^{r} M_lc_l$, where the M_l's are distinct monomials in x_i's and y_j's and $0 \neq c_l \in C$. Since

$$\deg(f_1f_2\dots f_n) = \deg(f_1) + \deg(f_2) + \dots + \deg(f_n) = n - k,$$

there exists an index l_0 such that $M_{l_0} = Ny_{i_1}y_{y_2}\dots y_{i_k}$, where N is a monomial in x_j's of degree $n-k$. Recall that $f_{i_t} = y_{i_t}$ and $f_{s_j} = x_j$ for all $t = 1, 2, \dots, k$, $j = 1, 2, \dots, m$. Hence $\deg_{x_j}(N) \leq n-k-(m-1) = n+1-k-m$. By our assumptions either $char(R) = 0$, or $char(R) > n+1-k-m$. Therefore $\phi(N) \in \mathcal{W}_0$ and so $|\phi(N)| = n-k$. It follows from **(ii)** that $|d_1d_2\dots d_n| = |\phi(N)| = n-k$ and the lemma is proved.

The following theorem is due to Chebotar [78].

Theorem 7.9.14 *Let R be a prime ring with extended centroid C and $d_1, d_2, \dots, d_n \in D = D(R)\setminus\{0\}$ where $n > 1$. Further let $d_{i_1}, d_{i_2}, \dots, d_{i_k}$, $1 \leq i_1 < i_2 < \dots < i_k \leq n$, be all the X-inner derivations from the set $\{d_1, d_2, \dots, d_n\}$ and let $d_{s_1}, d_{s_2}, \dots, d_{s_m}$, $1 \leq s_1 < s_2 < \dots < s_m \leq n$, be a maximal C-independent subset of $\{d_1, d_2, \dots, d_n\}$ modulo D_i. Suppose that $d_1d_2\dots d_n =$*

$d \in D(R)$ and either $char(R) = 0$, or $char(R) > n+1-k-m$. Then:

(i) $d \in D_i$;

(ii) If $char(R) \neq 2$, then $k \geq 3$;

(iii) If $k < n$, then $k > 0$ and $d_{i_1} d_{i_2} \dots d_{i_k} = 0$.

Proof. Setting $\mu_j = d_{s_j}$ for all $j = 1, 2, \dots, m$, we may choose a linearly ordered C-basis $\mathcal{B}_0$ of D modulo D_i such that $\mu_1 < \mu_2 < \dots < \mu_m \in \mathcal{B}_0$. We may also assume that $d = \sum_{j=1}^{q} \mu_j c_j + ad(a)$ for some $q \geq m$, $c_j \in C$, $a \in Q = Q_s(R)$ and $\mu_j \in \mathcal{B}_0$ for all $j = 1, 2, \dots, q$. Clearly $d_i = \sum_{j=1}^{m} \mu_j c_{ij} + ad(a_i)$ for some $c_{ij} \in C$, $a_i \in Q$ where $i = 1, 2, \dots, n$. It follows from (7.56) that

$$d = d_1 d_2 \dots d_n = \sum_{s=1}^{r} \Delta_s \Omega_s \tag{7.60}$$

where $\Delta_s \in \mathcal{W}_0$, and the Ω_s's belong to the right C-span of $C, \mathcal{B}_i, \mathcal{B}_i^2, \dots \mathcal{B}_i^n$. Here we note that if $k > 0$, then the Ω_s's belong to the right C-span of $\mathcal{B}_i, \mathcal{B}_i^2, \dots \mathcal{B}_i^n$. According to Lemma 7.9.13 **(i)** $|d| = n - k$ and so $|\Delta_s| \leq n - k$ for all s. Furthermore there exists at least one index s_0 such that $|\Delta_{s_0}| = n - k$ and $\Omega_{s_0} = d_{i_1} d_{i_2} \dots d_{i_k} h_{s_0}$ where $0 \neq h_{s_0} \in C$, and all Δ_s's with $|\Delta_s| = n - k$ appearing in (7.60) are distinct and are products of μ_j's (see Lemma 7.9.13 **(ii)**). Consider the following reduced T-identity on R:

$$\sum_{j=1}^{q} x^{\mu_j} c_j + [x, a] - \sum_{s=1}^{r} x^{\Delta_s \rho(\Omega_s)} \tag{7.61}$$

where $\rho : T_i \to End_C(S)$ is the C-algebra map introduced in section 7.2. By Theorem 7.7.9 we have that

$$\sum_{j=1}^{q} y_{\mu_j} c_j + [x, a] - \sum_{\Delta_s \neq 1} y_{\Delta_s}^{\rho(\Omega_s)} - \sum_{\Delta_s = 1} x^{\rho(\Omega_s)} \tag{7.62}$$

is a T-identity on Q. Only the following two cases are possible:

Case 1. Suppose that $k = n$. Then $\Delta_s = 1$ for all $s = 1, 2, \dots, r$. Setting $x = 0$, we conclude from (7.62) that $c_j = 0$ for all $j = 1, 2, \dots, q$ and so $d = ad(a) \in D_i$. Next suppose that $char(R) \neq 2$. Then in view of Theorem 7.9.12, $n \neq 2$. Since $n > 1$, we have that $k = n \geq 3$. Thus in this case the theorem is proved.

Case 2. Suppose that $k < n$. We claim that $k > 0$. Indeed, let $k = 0$. By Lemma 7.9.13 there exists at least one index s_0 such that $|\Delta_{s_0}| = n$ and $\Omega_{s_0} = h_{s_0} \in C$. Since $n > 1$ and $\Delta_s \in \mathcal{W}_0$, we see that $\Delta_{s_0} \neq \mu_j$ for all $j = 1, 2, \dots, q$. Now recall that $\Delta_{s_0} \neq \Delta_p$ for $p \neq s_0$. Sending to zero all the variables in (7.62) distinct from $y_{\Delta_{s_0}}$, we obtain that $y_{\Delta_{s_0}} h_{s_0}$ is a T-identity on Q, a contradiction. Thus $k > 0$ and our claim is established. It was noted that the relation $k > 0$ implies that all Ω_s's belong to the right C-span of $\mathcal{B}_i, \mathcal{B}_i^2, \dots, \mathcal{B}_i^n$. In particular in this case $1^{\Omega_s} = 0$ for all $s = 1, 2, \dots, r$. Pick any $1 \leq j \leq q$. Sending to zero all the variables in (7.62) distinct from y_{μ_j} we obtain that

$$y_{\mu_j} c_j - \sum_{\Delta_s = \mu_j} y_{\mu_j}^{\rho(\Omega_s)}.$$

Letting $y_{\mu_j} = 1$, we see that $c_j = 0$. Therefore $d = ad(a) \in D_i$ and (7.62) yields

$$[x, a] - \sum_{\Delta_s \neq 1} y_{\Delta_s}^{\rho(\Omega_s)} - \sum_{\Delta_s = 1} x^{\rho(\Omega_s)} \tag{7.63}$$

is a T-identity on Q. Since $k < n$, $|\Delta_{s_0}| = n - k > 0$. It follows from (7.63) that $y_{\Delta_{s_0}}^{\rho(\Omega_{s_0})} = 0$. Recalling that $d_{i_1} d_{i_2} \dots d_{i_k} = \Omega_{s_0} h_{s_0}^{-1}$, we conclude that the composition $d_{i_1} d_{i_2} \dots d_{i_k}$ of derivations is equal to zero. From Theorem 7.9.12 we infer that $k \geq 3$. The theorem is thereby proved.

The following theorem is due to Chuang [84].

Theorem 7.9.15 *Let R be a prime ring of characteristic $p > 0$ and $d_1, d_2, \dots, d_p \in D = D(R)$. Suppose that $d_1 d_2 \dots d_p = d \in D$. Then:*

(i) *If $\{d_1, d_2, \dots, d_p\} \cap D_i \neq \emptyset$, then $d \in D_i$;*

(ii) *If $\{d_1, d_2, \dots, d_n\} \cap D_i = \emptyset$, then $d_j \in d_1 C + D_i$ for all $j = 2, 3, \dots, p$ and there exists $c \in C$ such that $d = d_1^p c$.*

Proof. If $|\{d_1, d_2, \dots, d_p\} \cap D_i| = k > 0$, then $char(R) = p > p - k$ and so Theorem 7.9.14 is applicable. Therefore $d \in D_i$. Next suppose that $\{d_1, d_2, \dots, d_p\} \cap D_i = \emptyset$. Let $V = \sum_{i=1}^{p} d_i C$ and $m = \dim_C((V + D_i)/D_i)$. If $m > 1$, then $char(R) = p > p + 1 - m$ and so by Theorem 7.9.14 **(iii)** we have that $\{d_1, d_2, \dots, d_p\} \cap D_i \neq \emptyset$, a contradiction. Therefore $m = 1$ and so $d_i \in d_1 C + D_i$. For simplicity we set $\delta = d_1$. Then $d_i = \delta c_i + ad(a_i)$ for some $0 \neq c_i \in C$, $a_i \in Q$, where $i = 2, 3, \dots, p$. We set $\nu_1 = \delta$. Let ν_i be equal to either δc_i or $ad(a_i)$, where $i = 2, 3, \dots, p$. Consider the product $\nu = \nu_1 \nu_2 \dots \nu_p$. If at least one of the ν_i's is X-inner, then $\nu = \sum_{j=1}^{p-1} \delta^j \Omega_j$ where the Ω_j's belong to the right C-span of $\mathcal{B}_i, \mathcal{B}_i^2, \dots, \mathcal{B}_i^{p-1}$. On the other hand if $\nu_i = \delta c_i$ for all $i = 2, 3, \dots, p$, then

$$\nu = \delta \delta c_1 \delta c_2 \dots \delta c_p = \sum_{j=2}^{p} \delta^j \alpha_j$$

for some $\alpha_j \in C$. Therefore

$$d = \delta^p \alpha_p + \sum_{j=2}^{p-1} \delta^j \alpha_j + \sum_{j=1}^{p-1} \delta^j \Omega_j. \tag{7.64}$$

The following two cases are the only possible ones.

Case 1. δ and δ^p are C-independent modulo D_i. Then setting $\mu_1 = \delta$ and $\mu_2 = \delta^p$ we may choose a C-basis $\mathcal{B}_0$ of D modulo D_i such that $\mu_1, \mu_2 \in \mathcal{B}_0$. Clearly $d = \sum_{i=1}^{q} \mu_i r_i + ad(a)$ for some $\mu_3, \mu_4, \dots, \mu_q \in \mathcal{B}_0$, $r_i \in C$, $a \in Q$. Consider the following reduced T-identity on R:

$$\sum_{i=1}^{q} x^{\mu_i} r_i + [x,\, a] - x^{\mu_2}\alpha_p - \sum_{j=2}^{p-1} x^{\mu_1^j}\alpha_j - \sum_{j=1}^{p-1} x^{\mu_1^j \rho(\Omega_j)}.$$

It follows from Theorem 7.7.9 that

$$\sum_{i=1}^{q} y_{\mu_i} r_i + [x,\, a] - y_{\mu_2}\alpha_p - \sum_{j=2}^{p-1} y_{\mu_1^j}\alpha_j - \sum_{j=1}^{p-1} y_{\mu_1^j}^{\rho(\Omega_j)}$$

is a T-identity on Q. Now we conclude that $r_i = 0$ for all $i > 2$, $r_2 = \alpha_p$, $\alpha_j = 0$ for all $j = 2, 3, \ldots, p-1$, and $y_{\mu_1^j}^{\rho(\Omega_j)} = 0$ for all $j = 2, 3, \ldots, p-1$ (in particular $x^{\mu_1^j \rho(\Omega_j)} = 0$ for all $x \in Q$). Hence we see that

$$y_{\mu_1} r_1 + [x,\, a] - y_{\mu_1}^{\rho(\Omega_1)} \tag{7.65}$$

is a T-identity on Q. Sending y_{μ_1} to 1 and x to 0, we obtain that $r_1 = 0$. On the other hand, sending y_{μ_1} to zero we see that $[x,\, a]$ is a T-identity on Q and so $ad(a) = 0$. It follows from (7.65) that $y_{\mu_1}^{\rho(\Omega_1)} = 0$. Summarizing what we have proved, we conclude that $d = \mu_2\alpha_p = \delta^p\alpha_p$.

Case 2. $\delta^p = \delta c + ad(b)$ for some $0 \neq c \in C$ and $a \in Q$. We set $\mu_1 = \delta$ and we may assume that $\mu_1 \in \mathcal{B}_0$. Then one can show that $d = \mu_1 r + ad(a)$ for some $r \in C$, $a \in Q$, and $x^{\mu_1^j \rho(\Omega_j)} = 0 = \alpha_j$ for all $j = 2, 3, \ldots, p-1$, and (7.64) yields the following T-identity on Q:

$$y_{\mu_1} r + [x,\, a] - y_{\mu_1} c\alpha_p - [x,\, b]\alpha_p - y_{\mu_1}^{\rho(\Omega_1)}.$$

Sending y_{μ_1} to 0 we see that $[x,\, a] = [x,\, b]\alpha_p$. On the other hand, sending x to 0 and y_{μ_1} to 1 we obtain that $r = c\alpha_p$. Now it follows that $y_{\mu_1}^{\rho(\Omega_1)} = 0$. Therefore $x^{\mu_1 \rho(\Omega_1)} = 0$ and so $d = \delta c\alpha_p + [x,\, b]\alpha_p = \delta^p\alpha_p$ thus proving the theorem.

We close this section with the following result of Lanski [168]

Theorem 7.9.16 *Let R be a prime ring of characteristic distinct from 2 with extended centroid C and $d_1, d_2, d_3 \in D = D(R)$. Suppose that $d_1 d_2 d_3 = d \in D$. Then either $d_1, d_2, d_3 \in D_i$, or $char(R) = 3$, $d_i = d_1 c_i$ for some $c_i \in C$, $i = 2, 3$, where $c_2^{d_1} = 0$.*

Proof. If either $char(R) = 0$ or $char(R) > 3$, then $d_1, d_2, d_3 \in D_i$ by Theorem 7.9.14. Suppose that $char(R) = 3$. First we consider the case $|\{d_1, d_2, d_3\} \cap D_i| = k > 0$. Then $char(R) = 3 > 3 - k$ and so by Theorem 7.9.14 we have $k = 3$. Next suppose that $k = 0$. Then $d_1, d_2, d_3 \notin D_i$. Now it follows from Theorem 7.9.15 that $d_2 = d_1 u + ad(a)$ and $d_3 = d_1 v + ad(b)$ for some $0 \neq u, v \in C$, $a, b \in Q$. Setting for simplicity $\delta = d_1$ we see that

$$\begin{aligned} d &= d_1 d_2 d_3 = \delta(\delta u + ad(a))(\delta v + ad(b)) \\ &= \delta^3 uv + \delta^2 u^\delta v + \delta^2 ad(a)v + \delta ad(a^\delta)v \\ &\quad + \delta^2 ad(b)u + \delta ad(a)ad(b) \end{aligned}$$

By Theorem 7.9.15**(ii)** we have $d = \delta^3 c$, $c \in C$, and so

$$\delta^3(c-uv)-\delta^2(u^\delta v+ad(a)v+ad(b)u)-\delta(ad(a^\delta)v+ad(a)ad(b)) = 0 \tag{7.66}$$

We claim that there exists $\gamma \in C$ such that

$$\gamma + ad(a^\delta)v + ad(a)ad(b) = 0 \tag{7.67}$$

$$u^\delta v + ad(av + bu) = 0 \tag{7.68}$$

Indeed, if δ, δ^3 are C-independent $modD_i$ we may assume $\delta, \delta^3 \in \mathcal{B}_0$. Then the T-identity determined by (7.66) is reduced and so by Theorem 7.5.6 (7.67) and (7.68) hold (taking $\gamma = 0$). Otherwise we substitute $\delta^3 = \delta\beta + ad(g)$, $\beta \in C$, $g \in Q$, into (7.66), and from the resulting reduced identity we see again by Theorem 7.5.6 that (7.67) and (7.68) hold (taking $\gamma = -\beta(c - uv)$). Applying (7.67) to 1 we see that $\gamma = 0$, whence by Theorem 7.9.12 either $a \in C$ or $b \in C$. On the other hand applying

(7.68) to 1 results in $u^\delta v = 0$ and so $u^\delta = 0$. But this forces $av + bu \in C$ and since $u, v \neq 0$, we conclude that both a and b lie in C. Thus $d_2 = d_1 u$, $d_3 = d_1 v$, and $u^{d_1} = u^\delta = 0$, which completes the proof.

Chapter 8

$\widehat{T}$-identities of Semiprime Rings

The aim of the present chapter is to prove for semiprime rings the results analogous to the main theorems for prime rings with T-identities (see Chapter 7).

We first set in place some notations. Throughout this chapter R will be a semiprime ring with extended centroid C, $Q = Q_{mr}(R)$, $S = O(R)$ the orthogonal completion of R, $Q_s = Q_s(S)$ and $B = B(C)$. Further D_i will be the Lie algebra of inner derivations of Q_s, $D = D(R) = Der(S)C + D_i$, G_i the X-inner automorphisms of S, and $G = G(R) = Aut(S) \cup Antiaut(S)$. Further let $M \in Spec(B)$ and let $\phi_M : Q \to \overline{Q} = Q/MQ$ be the canonical surjection of rings. We set

$$\overline{S} = \phi_M(S),\ \overline{Q_s} = \phi_M(Q_s), \quad \text{and} \quad \overline{C} = \phi_M(C).$$

We already know that $\overline{S}$ is a prime ring with extended centroid $\overline{C}$, $\overline{Q} \subseteq Q_{mr}(\overline{S})$ and $\overline{Q_s} \subseteq Q_s(\overline{S})$ by Theorem 3.2.7 and Theorem 3.2.15.

The first problem which we have to overcome is that in the semiprime ring case the universal enveloping algebra $U(D(R))$ of the differential C-Lie algebra $D(R)$ is not working as well as in the prime ring case. The reasons are the following. First of all it is easy to see that $D(R)$ is not a restricted Lie algebra in general, but it may have some direct summands of the form $eD(R)$, $e \in B$, which are restricted differential eC-Lie algebras. In the first section we construct a *reduced* enveloping algebra $\widehat{U}(D(R))$ which reflects this situation. Next the algebra $\widehat{U}(D(R))$ has no PBW basis because $D(R)$ is not a free right C-module in general. But we show that this algebra locally has a basis of PBW type. The second problem is that in the semiprime ring case the group $G(R)$ does not serve our needs as well as in the prime ring case. In the second section we construct a larger group $\widehat{G}(R)$ and discuss its properties. The first two sections form a base for the notion of a *reduced* T-identity on an ideal of a semiprime ring which is introduced and discussed in third section. The last section is devoted to proofs of the analogs of the results in Chapter 7 about prime rings with T-identities.

8.1 The Algebra $\widehat{U}(D(R))$

Let R be a semiprime ring, let $\mathcal{P}$ be the set of all prime numbers and let $\mathcal{P}_0 = \mathcal{P} \cup \{0\}$. Setting $I_p = \{r \in R \mid pr = 0\}$, $p \in \mathcal{P}$, and $I_0 = r_R(\sum_{p\in\mathcal{P}} I_p)$, we note that $I = \sum_{p\in\mathcal{P}_0} I_p = \oplus_{p\in\mathcal{P}_0} I_p$ is a dense ideal of R and the additive group of I_0 is torsionfree. We leave it to the reader as an easy exercise to show that $Q_s = Q_s(I) = \prod_{p\in\mathcal{P}_0} Q_s(I_p)$ and $Q_s(I_p)^\mu, Q_s(I_p)^\alpha \subseteq Q_s(I_p)$ for all $\mu \in D$, $\alpha \in G$, $p \in \mathcal{P}_0$. Letting e_p denote the identity of $Q_s(I_p) \subseteq Q_s$, we remark that $\{e_p \mid p \in \mathcal{P}_0\}$ is a dense orthogonal subset of B and $e_p^\alpha = e_p$ for all $\alpha \in G$, $p \in \mathcal{P}_0$. Clearly $pQ_s(I_p) = 0$ and $Q_s(I_p) = e_pQ_s$ for all $p \in \mathcal{P}_0$. We note the following important property of the e_p's, the proof of which we leave to the reader. Let $M \in Spec(B)$. Then, for $p \in \mathcal{P}_0$,

$$char(C/MC) = p \quad \text{if and only if} \quad e_p \notin M. \tag{8.1}$$

Next recall that $v^\mu = 0$ for all $v \in B$, $\mu \in D$. Therefore $(xv)^\mu = x^\mu v = x^{\mu v}$ for all $x \in Q_s$. In particular

$$(Q_s(1-e_p))^{\mu e_p} = 0 \quad \text{and} \quad (Q_s)^{\mu e_p} \subseteq Q_s e_p$$

for all $p \in \mathcal{P}_0$. Since $pQ_s e_p = 0$, we infer from Remark 1.1.1(**b**) that $(\mu e_p)^p \in D$ for all $p \in \mathcal{P}$. Further the commutation formula (5.22) was proved for prime rings, but the same proof is valid also for semiprime rings. Therefore in $End(Q_s)$ the following formula holds:

$$c\delta = \delta c + c^{\widehat{\delta}}, \quad \delta \in D,\ c \in C, \tag{8.2}$$

where $\widehat{\delta}$ is the restriction of the derivation δ on C. Letting Φ_p denote the prime subfield of e_pC, we infer from Lemma 5.2.1(**c**) that e_pD is a special restricted differential e_pC-Lie algebra over Φ_p with cover $End(e_pQ_s)$, $p \in \mathcal{P}$.

Now let Φ be the subring of C generated by the identity. We note that $\Phi_p = e_p\Phi$ for all $p \in \mathcal{P}$. We identify the ring C with the subring $id_{Q_s}C$ of $End(Q_s)$ and set $\widehat{D} = C + D$. We claim that $D \cap C = 0$. Indeed, suppose that $\mu = c$ where $\mu \in D$, $c \in C$. Then

$$xyc = (xy)^\mu = x^\mu y + xy^\mu = (xc)y + x(yc) = 2xyc \quad \text{and} \quad xyc = 0$$

for all $x, y \in R$. Therefore $R^2c = 0$ and so $c = 0$ because R^2 is a dense ideal of R. Thus our claim is established and so $\widehat{D} = C \oplus D$. From (8.2) we conclude that $\widehat{D}$ is a special differential C-Lie algebra over Φ with cover $End(Q_s)$. According to Lemma 5.4.2(**c**) $e_p\widehat{D}$ is a restricted differential e_pC-Lie algebra over Φ_p with cover $End(e_pQ_s)$ for all $p \in \mathcal{P}$. Thus we have proved the following

Remark 8.1.1 *$\widehat{D}$ is a special differential C-Lie algebra over Φ with cover $End(Q_s)$. Moreover $e_p\widehat{D}$ is a restricted differential e_pC-Lie algebra over Φ_p with cover $End(e_pQ_s)$ for all $p \in \mathcal{P}$.*

Let $\mathcal{Z}$ be the ring of integers and $X = \{\overline{x} \mid x \in \widehat{D}\}$. We consider the ideal $I = I(\widehat{D})$ of $F = \mathcal{Z}{<}X{>}$ generated by all elements of the following forms:

$$\begin{aligned}
&(1)\ 1_F - \overline{1_C};\\
&(2)\ \overline{x} + \overline{y} - \overline{x+y} \quad \text{for all} \quad x, y \in \widehat{D};\\
&(3)\ \overline{x}\,\overline{c} - \overline{xc} \quad \text{for all} \quad x \in \widehat{D},\ c \in C;\\
&(4)\ [\overline{x}, \overline{y}] - \overline{[x, y]} \quad \text{for all} \quad x, y \in \widehat{D};\\
&(5)\ \overline{x}^p - \overline{x^p} \quad \text{for all} \quad x \in e_p\widehat{D},\ p \in \mathcal{P}.
\end{aligned}$$

Setting $\widehat{U} = \widehat{U}(D(R)) = F/I$ we note that the mapping $C \to \widehat{U}$ given by the rule $c \mapsto \overline{c} + I$, $c \in C$, is a homomorphism of rings with identity by **(1)**–**(3)**. Therefore $\widehat{U}$ is a C-ring. From **(4)** it follows that the mapping $\rho : \widehat{D} \to \widehat{U}$ given by $x \mapsto \overline{x} + I$, $x \in \widehat{D}$, is a homomorphism of Lie rings. Moreover by **(3)** ρ is a homomorphism of right C-modules. According to **(4)** we have

$$\rho\left(c^{\widehat{\delta}}\right) = \rho([c, \delta]) = [\overline{c}, \overline{\delta}] \subseteq 1 \cdot C$$

for all $c \in C$, $\delta \in D$. Now it follows that $\rho(\widehat{D})$ is a special differential C-Lie algebra over Φ with cover $\widehat{U}$ and ρ is a homomorphism of differential C-Lie algebras. Moreover by **(5)** $\rho : e_p\widehat{D} \to e_p\widehat{U}$ is a homomorphism of restricted differential e_pC-Lie algebras. Finally we note that the C-ring $\widehat{U}$ is generated by $\rho(D(R))$ and 1 according to **(1)**.

Our next goal is to show that ρ is an injection. To this end we set

$$N(B) = \{\tau \in End(Q_s) \mid \tau e = e\tau \quad \text{for all} \quad e \in B\}.$$

Let $M \in Spec(B)$ and let $\phi_M : Q_s \to \overline{Q_s} = Q_s/MQ_s$ be the canonical surjection of C-algebras. Since $\tau(MQ_s) = M\tau(Q_s)$ for all $\tau \in N(B)$, we conclude that τ induces an endomorphism $\widetilde{\tau}$ of the additive group of $\overline{Q_s}$. Clearly the mapping $\psi_M : N(B) \to End(\overline{Q_s})$ given by $\psi_M(\tau) = \widetilde{\tau}$, $\tau \in N(B)$, is a homomorphism of C-rings.

Remark 8.1.2 *The following conditions are fulfilled:*

(i) *$N(B)$ is a nonsingular right C-module;*

(ii) *D_i is an injective submodule of the C-module $N(B)$. In particular D_i is an orthogonally complete subset of $N(B)$;*

(iii) $\ker(\psi_M) = MN(B) = \{\tau \in N(B) \mid E(\tau) \in M\}$;

(iv) $\psi_M(\widehat{D}) \subseteq \phi_M(C) + D(\phi_M(S)) \subseteq End(Q_s(\phi_M(S)))$;

(v) $\psi_M : \widehat{D}(R) \to \phi_M(C) + D(\phi_M(S)) = \widehat{D}(\phi_M(S))$ *is a homomorphism of differential C-Lie algebras;*

(vi) *If $e_p \notin M$, then $\psi_M(\widehat{D}) = \psi_M(\widehat{D}e_p)$ and $\psi_M : \widehat{D}e_p \to \phi_M(C)+D(\phi_M(S))$ is a homomorphism of restricted differential e_pC-Lie algebras.*

Proof. **(i)** It follows directly from the definition of $N(B)$ that it is a C-submodule of $End(Q_s)$. Clearly $r_C(\tau) = r_C(Q_s^\tau) = (1 - E(Q_s^\tau))C$ by Theorem 2.3.9(**i**) for all $\tau \in N(B)$. Therefore $N(B)$ is a nonsingular C-module and $E(\tau) = E(Q_s^\tau)$.

(ii) Clearly D_i is a C-submodule of $N(B)$. By Proposition 3.1.10 D_i is orthogonally complete. It follows from Proposition 3.1.6 that D_i is an injective C-module.

(iii) The equality $MN(B) = \{\tau \in N(B) \mid E(\tau) \in M\}$ is proved similarly to Remark 3.2.2(**ii**). Assume that $\widetilde{\tau} = 0$ where $\tau \in N(B)$. Then $\phi_M(Q_s^\tau) = 0$. By Lemma 3.1.18 Q_s^τ is an orthogonally complete subset of Q_s. Now it follows from Corollary 3.2.4(**iii**) that $E(\tau) = E(Q_s^\tau) \in M$. On the other hand if $E(\tau) \in M$, then $\phi_M(Q_s^\tau) = 0$ by Corollary 3.2.4(**iii**) and so $\tau \in \ker(\psi_M)$.

Noting that $\overline{Q_s} \subseteq Q_s(\phi_M(S))$ by Theorem 3.2.15(**iii**), we leave it for the reader to check the straightforward details of **(iv)**–**(vi)**.

Consider now the universal enveloping algebra $(U(D(\overline{S})); \chi)$ of the (restricted) differential $\overline{C}$-Lie algebra $D(\overline{S})$. As we already know $\overline{C}$ is a field. By Corollary 5.3.7 and Corollary 5.4.6 χ is a monomorphism. Clearly $D(\overline{S})^\chi \subseteq U(D(\overline{S}))$ is a special differential $\overline{C}$-Lie algebra. We identify $D(\overline{S})$ and $D(\overline{S})^\chi$

via χ. From Lemma 5.4.2(**c**) it follows that all the conditions of Definition 5.3.1 and Definition 5.4.1 hold for $\overline{C} + D(\overline{S})$ and so it is a special (restricted) differential $\overline{C}$-Lie subalgebra of $U(D(\overline{S}))$. Clearly $\overline{C} + D(\overline{S})$ is a special (restricted) differential C-Lie subalgebra of $U(D(\overline{S}))$ as well. Define the mapping $\alpha_M : \widehat{D} \to \overline{C} + D(\overline{S})$ by the rule $\alpha_M(c+\mu) = \phi_M(c) + \psi_M(\mu)$ for all $\mu \in D(R)$, $c \in C$. Clearly α_M is a homomorphism of differential C-Lie algebras. It follows directly from the definition of $\widehat{U}$ that there exists a unique homomorphism $\Psi_M : \widehat{U} \to U(D(\overline{S}))$ of C-rings such that $\alpha_M = \Psi_M \rho$. Therefore

$$\ker(\rho) \subseteq \cap_{M \in Spec(B)} \ker(\alpha_M).$$

Clearly $\ker(\alpha_M) = \ker(\phi_M) \oplus \ker(\psi_M)$. It follows that

$$\begin{aligned} \cap_{M \in Spec(B)} \ker(\alpha_M) &= (\cap_{M \in Spec(B)} \ker(\phi_M)) \\ &\quad \oplus (\cap_{M \in Spec(B)} \ker(\psi_M)) = 0 \end{aligned}$$

by Remark 8.1.2(**iii**). Thus we have proved the following

Corollary 8.1.3 *The mapping $\rho : \widehat{D} \to \widehat{U}(\widehat{D})$ is a monomorphism.*

In what follows we shall identify (via ρ) C and D with $\rho(C)$ and $\rho(D)$ respectively. We shall call $\widehat{U}(D(R))$ the *reduced* universal enveloping algebra of the differential C-Lie algebra $D(R)$.

Lemma 8.1.4 *Let $\delta \in D(R)$ be such that $0 \neq \psi_M(\delta) \in D_i(\overline{S})$. Then there exist elements $a_1, a_2, b \in S$ such that $E(a_1) = E(a_2) = E(b) \notin M$ and $bx^\delta b + a_1 x b + b x a_2 = 0$ for all $x \in Q_s$.*

Proof. Let $\psi_M(\delta) = ad(q)$ where $q \in Q_s(\overline{S})$. Clearly $Iq + qI \subseteq \overline{S}$ for some nonzero ideal I of $\overline{S}$. Suppose that for all $x \in I$ either $qx = 0$ or $xq = 0$. According to Proposition 2.2.1 $L = qI \neq 0$. It follows that $y^2 = 0$ for all $y \in L$. We have

$$0 = (y+z)^2 = y^2 + yz + zy + z^2 = yz + zy \quad \text{and} \quad yz = -zy$$

for all $y, z \in L$. Therefore $(yz)(yt) = y(zy)t = -y^2zt = 0$ for all $y, z, t \in L$ and so $(yL)^2 = 0$. By Theorem 3.2.7 $\overline{S}$ is a prime ring and hence $yL = 0$ for all $y \in L$. It follows that $L^2 = 0$ which implies that $L = 0$, a contradiction. Therefore $dq \neq 0 \neq qd$ for some $d \in I$. We choose $b', a_1', a_2' \in S$ such that $\phi_M(b') = d$, $\phi_M(a_1') = dq$ and $\phi_M(a_2') = -qd$. Consider the mapping $\tau : S \to S$ given by $x^\tau = b'x^\delta b' + a_1'xb' + b'xa_2'$, $x \in S$. Since $dx^{ad(q)}d + dqxd - dxqd = 0$ for all $x \in \overline{S}$, we conclude that $\phi_M(S^\tau) = 0$. By Lemma 3.1.18 S^τ is an orthogonally complete subset of S. Now it follows from Corollary 3.2.4(**iii**) that $vS^\tau = 0$ for some $v \in B \setminus M$. Since d, qd, dq are nonzero elements, we infer from Corollary 3.2.4(**ii**) that $e = vE(b')E(a_1')E(a_2') \notin M$. We set $b = eb'$, $a_1 = ea_1'$ and $a_2 = ea_2'$. From $eS^\tau = 0$ we conclude that $bx^\delta b + a_1xb + bxa_2 = 0$ for all $x \in S$. It follows from Theorem 2.3.9(**ii**) that $e = E(b) = E(a_1) = E(a_2)$. The proof is complete.

Given $\delta \in D(R)$, we recall from section 3.1 that

$$M_\delta = \{m \in Q \mid \delta E(m) = ad(m)\}.$$

Lemma 8.1.5 *Let $\delta \in D(R)$ and $a_1, a_2, b \in S$ be such that $E(a_1) = E(a_2) = E(b) = e$ and*

$$bx^\delta b + a_1xb + bxa_2 = 0 \quad \textit{for all} \quad x \in Q_s. \tag{8.3}$$

Then there exists an element $q \in Q_s$ such that $E(q) \leq e$ and $\delta e = ad(q)$. In particular $q \in M_\delta$.

Proof. We define the mapping $\tau : SbS \to S$ by the rule $b \cdot \beta \mapsto b \cdot \beta^\delta + a_2 \cdot \beta$, $\beta \in S^\circ \otimes_C S$. Suppose $b \cdot \beta = 0$ for some $\beta = \sum r_i \otimes s_i \in S^\circ \otimes_C S$. Substituting xr_i for x in (8.3) and multiplying by s_i from the right, we obtain

$$bx^\delta r_ibs_i + bxr_i^\delta bs_i + a_1xr_ibs_i + bxr_ia_2s_i = 0$$

for all $x \in S$. Since $b \cdot \beta = 0$, we have

$$0 = bx(b \cdot \beta^\delta) + bx(a_2 \cdot \beta) = bx(b \cdot \beta^\delta + a_2 \cdot \beta)$$

for all $x \in S$. According to Lemma 2.3.10 we have that

$$\begin{aligned} 0 &= E(b)(b \cdot \beta^\delta + a_2 \cdot \beta) \\ &= (E(b)b) \cdot \beta^\delta + (E(b)a_2) \cdot \beta \\ &= b \cdot \beta^\delta + a_2 \cdot \beta \end{aligned}$$

since $E(b) = E(a_2)$. Therefore the mapping τ is well-defined. Clearly τ is a homomorphism of right S-modules. By Proposition 2.2.1(**iv**) there exists an element $q' \in Q_r = Q_r(S)$ such that $x^\tau = q'x$ for all $x \in SbS$. Let $t \in S$ and $\beta \in S^\circ \otimes_C S$. We set $\gamma = \beta(t \otimes 1)$. We have

$$\begin{aligned} q't(b \cdot \beta) &= q'(b \cdot \gamma) = (b \cdot \gamma)^\tau = b \cdot \gamma^\delta + a_2 \cdot \gamma \\ &= t^\delta(b \cdot \beta) + t(b \cdot \beta^\delta) + t(a_2 \cdot \beta) \\ &= t^\delta(b \cdot \beta) + tq'(b \cdot \beta) \end{aligned}$$

and so

$$([q', t] - t^\delta)SbS = 0$$

for all $t \in S$. It follows from Lemma 2.3.10 that

$$([q', t] - t^\delta)E(SbS) = 0.$$

Since $r_C(SbS) = r_C(b)$, we obtain that $E(SbS) = E(b)$. Setting $q = -q'E(b)$ we conclude that $ad(q) = \delta E(b)$ (whence $q \in Q_s$). We recall from Theorem 2.3.9(**ii**) that $E(q) = E(b)E(q') \leq e = E(b)$. Finally we note that $E(ad(q)) \leq E(q) \leq e$ and so $\delta E(q) = \delta e E(q) = ad(q)E(q) = ad(q)$. Thus $q \in M_\delta$ and the proof is complete.

Corollary 8.1.6 *Let $\delta \in D(R)$ and $P \in Spec(B)$. Then*

$$\phi_P(M_\delta) = M_{\psi_P(\delta)}.$$

Proof. First of all we note that $0 \in M_\delta$ since $0 = ad(0) = \delta 0 = \delta E(0)$. Let $m \in M_\delta$. If $E(m) \in P$, then $\psi_P(ad(m)) = 0 \in M_{\psi_P(\delta)}$. If $E(m) \notin P$, then $\psi_P(ad(m)) = \psi_P(\delta E(m)) = \psi_P(\delta)$ and so $\phi_P(m) \in M_{\psi_P(\delta)}$. Therefore $\phi_P(M_\delta) \subseteq M_{\psi_P(\delta)}$. Suppose that $\phi_P(M_\delta) = 0$ but $M_{\psi_P(\delta)} \neq 0$. From Lemma 8.1.4 it follows that the conditions of Lemma 8.1.5 are fulfilled with $E(b) = e \notin P$. By Lemma 8.1.5 we conclude that $\delta e = ad(q)$ for some $q \in M_\delta$. According to our assumption $\phi_P(q) = 0$. Therefore

$$\psi_P(\delta) = \psi_P(\delta e) = \psi_P(ad(q)) = ad(\phi_P(q)) = 0$$

and so $E(\delta) \in P$ by Remark 8.1.2(**iii**). Setting $v = 1 - E(\delta)$ we note that $v \notin P$ and $\delta v = 0$. Therefore $Cv \subseteq M_\delta$ and hence

$$0 \neq \phi_P(C) = \phi_P(Cv) \subseteq \phi_P(M_\delta) = 0,$$

a contradiction. Now assume that $\phi_P(M_\delta) \neq 0$. Let $0 \neq a = \phi_P(q)$ where $q \in M_\delta$ and $b \in M_{\psi_P(\delta)}$. Clearly $[x, b-a] = 0$ for all $x \in \phi_M(S)$. Therefore $b - a \in \phi_P(C)$ by Theorem 3.2.15(**iv**). Pick $c \in C$ such that $\phi_P(c) = b - a$. Since $(q + cE(q))E(q) = q + cE(q)$, we conclude that $E(q + cE(q)) \leq E(q)$. Clearly

$$ad(q + cE(q)) = ad(q) = \delta E(q)$$

and so

$$ad(q + cE(q)) = ad(q + cE(q))E(q + cE(q)) = \delta E(q + cE(q)).$$

It follows that $q + cE(q) \in M_\delta$. Next since $\phi_P(q) = a \neq 0$, $E(q) \notin P$. Therefore $\phi_P(q + cE(q)) = a + \phi_P(c) = b$ and so $\phi_P(M_\delta) = M_{\psi_P(\delta)}$. The proof is complete.

We are now in a position to fulfill the main goal of this section (Lemma 8.1.7 and Proposition 8.1.8). These results will show that $\widehat{U}(D(R))$ has "local" PBW-type bases which are "compatible" with the PBW bases of $U(D(\overline{S}))$ for various prime homomorphic images $\overline{S}$ of $S = O(R)$.

Let $\mathcal{M} = \{\mu_i \mid 1 \le i \le n\} \subseteq D(R)$. The set $\mathcal{M}$ is said to be *strongly independent* if for all $c_i \in C$, $1 \le i \le n$, the relation $\sum_{i=1}^n \mu_i c_i \in D_i$ implies that $\mu_i c_i = 0$ for all $i = 1, 2, \dots, n$. Obviously $\mathcal{M}$ is strongly independent if and only if $\sum_{i=1}^n \mu_i C = \oplus_{i=1}^n \mu_i C$ and $(\sum_{i=1}^n \mu_i C) \cap D_i = 0$. The notion of strong independence is of course motivated by the fact that in the special case when R is a prime ring $\mu_1, \mu_2, \dots, \mu_n \in D(R)$ are strongly independent if and only if they belong to some $\mathcal{B}_0(R)$ (see section 5.5).

Given a number $m > 0$ a product $\Delta = \mu_{i_1}\mu_{i_2}\dots\mu_{i_m} \in \widehat{U}$, $\mu_{i_k} \in \mathcal{M}$, is called a monomial in $\mathcal{M}$ of degree m. The monomial Δ is said to be *correct* if $i_1 \le i_2 \le \dots \le i_m$ and for every $p \in \mathcal{P}$, $p \le m$, the relations $e_p\mu_{i_k} \ne 0$ and $\mu_{i_k} = \mu_{i_{k+1}} = \dots = \mu_{i_{k+s-1}}$, where $k + s - 1 \le m$, imply that $s < p$.

Lemma 8.1.7 *Let $\mathcal{M} = \{\mu_i \mid 1 \le i \le n\} \subseteq D(R)$ be a strongly independent subset of derivations, $t, m > 0$ natural numbers, $\mathcal{D} = \{\Delta_j \mid 1 \le j \le t\}$ a set of pairwise distinct correct monomials in $\mathcal{M}$ of degree $\le m$, $P \in Spec(B)$, $\phi_P : Q \to \overline{Q} = Q/MQ$, $\psi_P : \widehat{D}(R) \to \widehat{D}(\overline{S})$ and $\Psi_P : \widehat{U}(D(R)) \to U(D(\overline{S}))$ the canonical homomorphisms. Then:*

(i) *There exists a basis $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_i$ of $D(\overline{S})$ such that*

$$\mathcal{D}' = \{\Psi_P(\Delta) \mid \Delta \in \mathcal{D} \quad \text{and} \quad \Psi_P(\Delta) \ne 0\} \subseteq \mathcal{W}_0,$$

where $\mathcal{W} = \mathcal{W}_0\mathcal{W}_i$ is a PBW-basis of $U(D(\overline{S}))$ (see section 5.4);

(ii) *If $\Delta_j = \mu_{ji_1}\mu_{ji_2}\dots\mu_{ji_k}$ where $k = k(j)$ and the μ_{ji_s}'s are in $\mathcal{M}$, then $r_C(\Delta_j) = (1 - E(\Delta_j))C$ where*

$$E(\Delta_j) = E(\mu_{ji_1})E(\mu_{ji_2})\dots E(\mu_{ji_k});$$

(iii) *$\sum_{j=1}^t \Delta_j C = \oplus_{j=1}^t \Delta_j C$.*

Proof. We recall from Theorem 3.2.7 and Theorem 3.2.15 that $\overline{S}$ is a prime ring with extended centroid $\overline{C}$. Further we claim that the set

$$\mathcal{M}' = \{\mu_i' = \psi_P(\mu_i) \mid 1 \le i \le n \quad \text{and} \quad \psi_P(\mu_i) \ne 0\}$$

is $\overline{C}$-independent modulo $D_i(\overline{S})$. Indeed, suppose to the contrary that $\sum \mu'_i\overline{c}_i = ad(y)$, $\mu'_i, \overline{c}_i \neq 0$, for some $y \in Q_s(\overline{S})$. In other words, setting $\mu = \sum \mu_i c_i$, we have $\psi_P(\mu) = ad(y)$ where $y \in M_{\psi_P(\mu)}$. By Corollary 8.1.6 $y = \phi_P(x)$, $x \in M_\mu$, whence $\sum \mu_i c_i E(x) = ad(x)$. Since the μ_i's are strongly independent, we have that $\mu_i c_i E(x) = 0$ for each i. As $\mu'_i\overline{c}_i \neq 0$ and $\mu'_i\overline{c}_i\phi_P(E(x)) = 0$, we conclude that $E(x) \in P$. Now from

$$\psi_P(\mu) = ad(y) = ad(\phi_P(x)) = \psi_P(ad(x))$$

we obtain $\mu = ad(x) + \tau$, where $\tau \in \ker(\psi_P)$. It follows that $E(\tau) \in P$. Clearly $e = (1 - E(x))(1 - E(\tau)) \notin P$ and $0 = \mu e = \sum \mu_i c_i e$. It follows that $\phi_P(e) = 1$ and each $\mu_i c_i e = 0$. Applying ψ_P we obtain the contradiction $\mu'_i\overline{c}_i = 0$ which proves our claim. Therefore there exists a linearly ordered basis $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_i$ of $D(\overline{S})$ such that $\mathcal{M}' \subseteq \mathcal{B}_0$ and $\mu'_i < \mu'_j$ if and only if $i < j$. If $char(\overline{C}) > m$ or $char(\overline{C}) = 0$, then clearly $\mathcal{D}' \subseteq \mathcal{W}_0$. Suppose that $char(\overline{C}) = p \leq m$. Then by (8.1) $e_p \notin M$ and so $\psi_P(e_p\mu_i) = \psi_P(\mu_i)$ for all $i = 1, 2, \ldots, n$. We conclude from the definition of correct monomials that $\mathcal{D}' \subseteq \mathcal{W}_0$.

It follows that $\Psi_P(\Delta_j) = 0$ if and only if $\psi_P(\mu_{ji_s}) = 0$ for some $1 \leq s \leq k$. We already know that $\psi_P(\mu_{ji_s}) = 0$ if and only if $E(\mu_{ji_s}) \in P$. Therefore $\Psi_P(\Delta_j) = 0$ if and only if

$$e = E(\mu_{ji_1})E(\mu_{ji_2})\ldots E(\mu_{ji_k}) \in P.$$

Let now $0 \neq c \in eC$. Then we choose $M \in Spec(B)$ such that $E(c) \notin M$. Clearly then $e \notin M$ and so $\Psi_M(\Delta_j c) = \Psi_M(\Delta_j)\phi_M(c) \neq 0$. Therefore $c \notin r_C(\Delta_j)$ and so $r_C(\Delta_j) \subseteq (1 - e)C$. On the other hand

$$\begin{aligned} \Delta_j E(\mu_{ji_s}) &= \mu_{ji_1}\ldots\mu_{ji_s}E(\mu_{ji_s})\ldots\mu_{ji_k} \\ &= \mu_{ji_1}\ldots\mu_{ji_s}\ldots\mu_{ji_k} = \Delta_j \end{aligned}$$

and hence $\Delta_j e = \Delta_j$. It follows that $r_C(\Delta_j) \supseteq (1 - e)C$ and therefore $r_C(\Delta_j) = (1 - e)C$, which shows that $E(\Delta_j) = E(\mu_{ji_1})E(\mu_{ji_2})\ldots E(\mu_{ji_k})$.

Suppose now that $\sum_{i=1}^{t} \Delta_j c_j = 0$ for some $c_1, c_2, \dots, c_t \in C$. Then $\sum_{j=1}^{t} \Psi_M(\Delta_j c_j) = 0$ and so $\Psi_M(\Delta_j c_j) = 0$ for all $j = 1, 2, \dots, t$ and $M \in Spec(B)$. Thus $\Delta_j c_j = 0$ and the proof is complete.

Proposition 8.1.8 *Let $\mathcal{M} = \{\mu_i \mid 1 \le i \le n\} \subseteq D(R)$ and $m > 0$ a natural number. Then there exist a strongly independent subset $\mathcal{M}_0 = \{\delta_j \mid 1 \le j \le t\} \subseteq D(R)$ and a subset $\mathcal{M}_i = \{\nu_k \mid 1 \le k \le s\} \subseteq D_i(R)$ such that any monomial Θ in $\mathcal{M}$ of degree $\le m$ is a right C-linear combination of products of the form $\Delta\Omega$, where Δ is a correct monomial in $\mathcal{M}_0$, Ω is a monomial in $\mathcal{M}_i$ and* $\deg(\Delta) + \deg(\Omega) \le \deg(\Theta)$.

Proof. We set $\mathcal{P}_m = \{p \in \mathcal{P} \mid p \le m\}$, $\mathcal{P}' = \mathcal{P}_m \cup \{0\}$, $v_p = e_p$, $p \in \mathcal{P}_m$, $v_0 = 1 - \sum_{p \in \mathcal{P}_m} e_p$ and

$$\mathcal{M}' = \{v_l \mu_i \mid 1 \le i \le n,\ l \in \mathcal{P}'\}.$$

Clearly any monomial of degree $l \le m$ in $\mathcal{M}$ is a sum of monomials in $\mathcal{M}'$ of the same degree. Furthermore any monomial in $\mathcal{M}'$ involving simultaneously $v_p \mu_i$ and $v_q \mu_j$ with $p \ne q \in \mathcal{P}'$ is equal to zero. Therefore it is enough to construct the desired subsets for each $\{v_l \mu_i \mid 1 \le i \le n, \}$, $l \in \mathcal{P}'$, provided that they will belong to $v_l D(R)$. Replacing S by $v_l S$ we reduce the proof to the following two cases:

Case 1 $pS = 0$ for some $p \le m$;

Case 2 $e_p = 0$ for all $p \in \mathcal{P}_m$.

We shall consider only the first case since in the second case the proof is virtually the same (but slightly simpler). Since $pS = 0$, $D(S)$ is a restricted differential C-Lie algebra over Φ_p.

By Remark 8.1.2 D_i is a direct summand of the right C-module D. Let $D = D_0 \oplus D_i$ and π_0, π_i be the projections on D_0 and D_i respectively. We set $K_1 = \sum_{i=1}^{n} \mu_i C$, $L_1 = \pi_0(K_1)$ and $N_1 = \pi_i(K_1)$. Clearly L_1 and N_1 are finitely generated nonsingular C-modules. It follows from Remark 3.1.4 that the

C-module L_1 has a strongly independent generating set $\mathcal{L}_1 = \{\delta_j \mid 1 \leq j \leq t_1\}$. We fix any finite generating set of the C-module N_1 and denote it by $\mathcal{N}_1$.

We proceed to construct by induction ordered 5-tuples $(K_i, L_i, \mathcal{L}_i, N_i, \mathcal{N}_i)$, $i = 2, 3, \ldots$, such that:

(a) K_i is a finitely generated right C-submodule of D containing K_{i-1};

(b) $L_i = \pi_0(K_i)$ and $\mathcal{L}_i = \{\delta_1, \delta_2, \ldots, \delta_{t_i}\}$ is a strongly independent generating set of L_i, where $t_i \geq t_{i-1}$;

(c) $N_i = \pi_i(K_i)$ and $\mathcal{N}_i$ is a finite generating set of the C-module N_i containing $\mathcal{N}_{i-1}$.

Suppose that we have already constructed a 5-tuple $(K_i, L_i, \mathcal{L}_i, N_i, \mathcal{N}_i)$. Then we set

$$K_{i+1} = L_i + N_i + \sum_{x,y \in \mathcal{L}_i \cup \mathcal{N}_i} [x, y]C + \sum_{x \in \mathcal{L}_i} x^p C.$$

Clearly K_{i+1} is finitely generated. Since $K_i \subseteq L_i + N_i$, we see that $K_i \subseteq K_{i+1}$. Next we set $L_{i+1} = \pi_0(K_{i+1})$ and $N_{i+1} = \pi_i(K_{i+1})$. Clearly L_{i+1} and N_{i+1} are finitely generated C-modules, $L_i \subseteq L_{i+1}$ and $N_i \subseteq N_{i+1}$. Choose any finite generating set $\mathcal{N}_{i+1}$ of N_{i+1} containing $\mathcal{N}_i$. Since L_i is an injective C-module (see Remark 3.1.4 and Theorem 2.3.9), $L_{i+1} = L_i \oplus L'$ for some submodule $L' \subseteq L_{i+1}$. According to Remark 3.1.4 the C-module L' has a strongly independent generating set, say, $\{\delta_{t_i+1}, \delta_{t_i+2}, \ldots, \delta_{t_{i+1}}\}$. Finally we set $\mathcal{L}_{i+1} = \{\delta_j \mid 1 \leq j \leq t_{i+1}\}$.

Next we prove by induction on m the following statement. For all $i = 1, 2, \ldots$ any monomial Θ in K_i of degree m is a right C-linear combination of products of the form $\Delta\Omega$, where Δ is a correct monomial in $\mathcal{L}_{i+m-1}$, Ω is a monomial in $\mathcal{N}_{i+m-1}$ and $\deg(\Delta) + \deg(\Omega) \leq m$.

If $m = 1$, then $\Theta = x \in K_i$. Since $K_i \subseteq L_i \oplus N_i$, we conclude that $x = \sum_{j=1}^{t_i} \delta_j c_j + \sum_{z \in \mathcal{N}_i} z d_z$ for some $c_j, d_z \in C$. Therefore our statement holds for $m = 1$. Suppose now that our statement holds for all $1 \leq k \leq m-1$. Writing elements involved in Θ as linear combinations of elements belonging to $\mathcal{L}_i \cup \mathcal{N}_i$ and using the commutation formula (5.22)

$$c\delta = \delta c + c^{\delta}, \quad \delta \in D,\ c \in C,$$

we obtain that Θ is a C-linear combination of monomials of the form $x_1 x_2 \ldots x_k$ where the x_j's belong to $\mathcal{L}_i \cup \mathcal{N}_i$ and $k \leq m$. It follows from the induction assumption that it is enough to consider only one such monomial $x_1 x_2 \ldots x_m$ of degree m. First assume that there exists an index j such that $1 \leq j \leq m-1$, $x_j \in \mathcal{N}_i$ and $x_{j+1} \in \mathcal{L}_i$. Clearly

$$\begin{aligned} x_1 x_2 \ldots x_m &= x_1 \ldots x_{j-1} x_{j+1} x_j x_{j+2} \ldots x_m \\ &\quad + x_1 \ldots x_{j-1}[x_j, x_{j+1}] x_{j+2} \ldots x_m. \end{aligned} \tag{8.4}$$

Since $x_1 \ldots x_{j-1}[x_j, x_{j+1}] x_{j+2} \ldots x_m$ is a monomial in K_{i+1} of degree $m-1$, we can apply the induction assumption. It follows that without loss of generality we may assume that there exists k such that $k \leq m$, $x_1, x_2, \ldots, x_k \in \mathcal{L}_i$ and $x_{k+1}, x_{k+2}, \ldots, x_m \in \mathcal{N}_i$. Next assume that there exists an index j such that $1 \leq j \leq k-1$, $x_j = \delta_r$, $x_{j+1} = \delta_s$ with $1 \leq s < r \leq t_i$. Then the equation (8.4) together with the induction assumption yields that without loss of generality we may assume that

$$x_1 = \delta_{j_1},\ x_2 = \delta_{j_2}, \ldots, x_k = \delta_{j_k}$$

with $j_1 \leq j_2 \leq \ldots \leq j_k$. Finally we note that the case when $j_l = j_{l+1} = \ldots = j_{l+p-1}$ is considered analogously. Therefore our statement is proved

Taking $\mathcal{M}_0 = \mathcal{L}_m$ and $\mathcal{M}_i = \mathcal{N}_m$ we complete the proof.

8.2 The Group $\widehat{G}(R)$

The following example shows that in the case of semiprime rings some new trivial T-identities appear.

Example Let A be any semiprime ring with 1. We set $R = A \oplus A \oplus A \oplus A$ and $e = (1, 1, 0, 0)$. Define automorphisms α and β of R by the rule

$$(a, b, c, d)^{\alpha} = (b, a, d, c),\ (a, b, c, d)^{\beta} = (b, a, c, d)$$

for all $(a, b, c, d) \in R$. Clearly $\alpha \neq \beta$ and $\phi(x) = ex^{\alpha} - ex^{\beta}$ is a T-identity on R.

At this point we note that the situation with the group $G(R)$ is in some sense analogous to that of $U(D(R))$: it does not work as well as in the prime ring case. We shall need to construct a larger group $\widehat{G}(R)$. To this end we recall that $End(Q_s)$ is a right C-module and for all $\gamma \in End(Q_s)$ we have $r_C(\gamma) = r_C(Q_s^{\gamma}) = (1 - E(Q_s^{\gamma}))C$ (see Theorem 2.3.9(**i**)). Therefore $End(Q_s)$ is a nonsingular C-module. Given a dense orthogonal subset $V \subseteq B$ and a subset $\{\gamma_v \mid v \in V\} \subseteq End(Q_s)$ we define a mapping $\gamma : Q_s \to Q_s$ by the rule $x^{\gamma} = \sum_{v \in V}^{\perp} x^{\gamma_v} v$ for all $x \in Q_s$. Clearly

$$x^{\gamma v} = x^{\gamma} v = x^{\gamma_v} v = x^{\gamma_v v}$$

for all $x \in Q_s$ and so $\gamma v = \gamma_v v$ for all $v \in V$. Noting that all that we have just shown is valid for $End(S)$ as well, we summarize these results in the following

Remark 8.2.1 *$End(Q_s)$ is a nonsingular orthogonally complete right C-module and $End(S)$ is an orthogonally complete subset of $End(Q_s)$.*

We consider $G(R)$ as a subgroup of $End(Q_s)$ and we identify C with $id_{Q_s}C$. Then the products αe and $e\alpha$ are defined, where $\alpha \in G(R)$, $e \in B$. Given $e \in B$, we may consider $End(eQ_s)$ as a subring of $End(Q_s)$ defining $x^t = (ex)^t$ for all $x \in Q_s$, $t \in End(eQ_s)$. We note that

$$End(eQ_s) = \{t \in End(Q_s) \mid et = t = te\}.$$

Since $eQ_s = Q_s(eS)$, by Proposition 2.5.3 and Proposition 2.5.4 we have

$$G(eS) \subseteq End(eQ_s).$$

The following remark will be especially useful when we come to defining "Frobenius elements".

Remark 8.2.2 *Let V be a dense orthogonal subset of B and*

$$g_v \in G(vS) \subseteq End(vQ_s) \subseteq End(Q_s),\ v \in V.$$

Suppose that $w^{g_v} = w$ for $v \in V$ and $w \in vB$. We set $g = \sum_{v\in V}^{\perp} g_v v$. Then:

(i) *g is an automorphism of additive groups of S and Q_s such that $e^g = e$ for all $e \in B$;*

(ii) *There exist orthogonal idempotents $u_1 = u_1(g), u_2 = u_2(g) \in B$ such that $u_1 + u_2 = 1$, $gu_1 \in Aut(u_1S) \subseteq Aut(u_1Q_s)$ and $gu_2 \in Antiaut(u_2S) \subseteq Antiaut(u_2Q_s)$;*

(iii) *If $g_v \in Aut(vS)$ for all $v \in V$, then $g \in Aut(S) \subseteq Aut(Q_s)$;*

(iv) *If $g_v \in Antiaut(vS)$ for all $v \in V$, then $g \in Antiaut(S) \subseteq Antiaut(Q_s)$;*

(v) *$g|_C$ is an automorphism of C.*

Proof. We shall prove **(i)**, **(iii)** and **(iv)** simultaneously. We show that g is an automorphism of the additive group of S. The case of Q_s is proved analogously. Let $x, y \in S$. Then

$$v(x+y)^g = [v(x+y)]^{g_v} = (vx)^{g_v}+(vy)^{g_v} = vx^g+vy^g = v(x^g+y^g)$$

for all $v \in V$ and so $(x+y)^g = x^g+y^g$ since V is a dense subset of B (see Theorem 2.3.9**(i)**). Here we note that if $g_v \in Aut(S)$ for all $v \in V$, then the equality $(xy)^g = x^g y^g$ is proved analogously. Now suppose that $x^g = 0$. Then $0 = x^g v = (vx)^{g_v}$ and so $vx = 0$ for all $v \in V$ which implies that $x = 0$. It follows that g is injective. Now let $z \in S$. Since g_v is either an automorphism or an antiautomorphism of vS, $vz = (y_v)^{g_v}$ for some $y_v \in vS$. It is not difficult to see that $y^g = z$ where $y = \sum_{v\in V}^{\perp} y_v v$. Therefore g is an automorphism of the additive group of S. Next since $e = \sum_{v\in V}^{\perp} ev$, we see that

$$e^g = \sum_{v\in V}{}^{\perp}(ev)^{g_v} = \sum_{v\in V}{}^{\perp} ev = e$$

and hence $e^g = e$ for all $e \in B$. Therefore **(i)**, **(iii)** and **(iv)** are proved.

(ii) We set $V_1 = \{v \in V \mid g_v \in Aut(vS)\}$, $V_2 = V \setminus V_1$, $u_1 = E(V_1)$ and $u_2 = E(V_2)$. Since $0 = V_1V_2S = V_1SV_2$, we infer from Lemma 2.3.10 that $E(V_1)E(V_2) = 0$ and so $u_1u_2 = 0$. We have $V = V_1 \cup V_2$, $v_1u_1 = v_1$ and $v_2u_2 = v_2$ for all $v_1 \in V_1$, $v_2 \in V_2$. Therefore $v(u_1+u_2) = v$ for all $v \in V$ and so $v(1-u_1-u_2) = 0$, $v \in V$. Recalling that V is a dense subset of B, we conclude that $u_1 + u_2 = 1$. Further $Vu_1 = V_1$ is a dense orthogonal subset of u_1B. Obviously $Q_s(u_1S) = u_1Q_s$, the extended centroid of u_1Q_s equals u_1C and $B(u_1C) = u_1B$. Finally $gu_1 = \sum_{v\in V}^{\perp} g_v v u_1 = \sum_{v\in V_1}^{\perp} g_v v$. By **(iii)** gu_1 is an automorphism of u_1S. Analogously one can show that gu_2 is an antiautomorphism of u_2S. The proof is complete.

Following section 7.6 we define an automorphism g of C to be Frobenius if either $g = 1$ or, in case $pC = 0$ for some prime p and $\theta : c \mapsto c^p$ is an automorphism of C, $g = \theta^n$ for some $n \in \mathcal{Z}$. Following section 7.7 we then define $g \in G(R)$ to be a Frobenius (anti)automorphism of S if the restriction $\widehat{g}$ of g to C is a Frobenius automorphism of C. We note that if g is a Frobenius (anti)automorphism, then $e^g = e$ for all $e \in B$. A mapping $g : S \to S$ is called a *Frobenius element* if there exist a dense orthogonal subset V of B and

$$\{g_v \mid g_v \quad \text{is a Frobenius (anti)automorphism of} \quad vS,\ v \in V\}$$

such that $g = \sum_{v\in V}^{\perp} g_v v$. Since any (anti)automorphism of vS has a unique extension to $vQ_s = Q_s(vS)$, we may assume that every g_v is an (anti)automorphism of vQ_s, $v \in V$. The following corollary follows immediately from Remark 8.2.2.

Corollary 8.2.3 *If g is a Frobenius element of $End(S)$, then g is an automorphism of the additive group of Q_s, $e^g = e$ for all $e \in B$, and g induces an automorphism of C.*

We denote by $G_f = G_f(R)$ the subset of all Frobenius elements of $End(S)$.

Proposition 8.2.4 *G_f is a subgroup of the multiplicative semigroup $End(Q_s)$ containing G_i and $\alpha^{-1}G_f\alpha = G_f$ for all $\alpha \in G(R)$.*

Proof. Let $g = \sum_{v\in V}^{\perp} g_v v$ and $h = \sum_{u\in U}^{\perp} h_u u$ be Frobenius elements. One can check that $f = gh = \sum_{v\in V,u\in U}^{\perp} g_v h_u vu$ and $g_v h_u$ is a Frobenius (anti)automorphism of vuS. Setting $W = VU$ and $f_w = g_v h_u$ for all $w = vu \in W$, $v \in V$, $u \in U$, we see that $f = \sum_{w\in W}^{\perp} f_w w$. As g_v is a Frobenius (anti)automorphism of vS, g_v^{-1} is a Frobenius (anti)automorphism of vS as well. Setting $h = \sum_{v\in V}^{\perp} g_v^{-1} v$ we note that h is a Frobenius element and

$$gh = \sum_{v\in V}{}^{\perp} g_v g_v^{-1} v = \sum_{v\in V}{}^{\perp} id_{vS} v = id_S.$$

Analogously $hg = id_S$ and so $g^{-1} = h \in G_f$. Therefore G_f is a subgroup of $End(Q_s)$. Obviously $G_i \subseteq G_f$. Finally let $\alpha \in G(R)$. We note that $e\alpha = \alpha e^{\alpha}$ for every $e \in B$. It follows that

$$\alpha^{-1} g\alpha = \sum_{v\in V}{}^{\perp} \alpha^{-1} g_v \alpha v^{\alpha}.$$

Since g_v is either a Frobenius automorphism or a Frobenius antiautomorphism of vS, $\alpha^{-1}g_v\alpha$ is respectively either a Frobenius automorphism or a Frobenius antiautomorphism of $v^{\alpha}S$. Noting that V^{α} is a dense orthogonal subset of B, we conclude that

$\alpha^{-1}g\alpha$ is a Frobenius element of $End(S)$ which completes the proof.

We set $\widehat{G}(R) = G(R)G_f(R)$ and continue with the following

Corollary 8.2.5 *$\widehat{G}(R)$ is a subgroup of $End(Q_s)$ and G_f, G_i are normal subgroups of $\widehat{G}(R)$.*

Proof. It follows from Proposition 8.2.4 that $\widehat{G}(R)$ is a subgroup of $End(Q_s)$ with the normal subgroup G_f. Since G_i is a normal subgroup of $G(R)$, it is enough to show that $f = g^{-1}inn(s)g \in G_i$ for all $g \in G_f$. Here we note that $e^f = e$ for all $e \in B$. Let $g = \sum_{v\in V}^{\perp} g_v v$ where V is a dense orthogonal subset of B and g_v is a Frobenius (anti)automorphism of vQ_s for all $v \in V$. We set $t_v = (vs)^{g_v}$ if g_v is an automorphism of vQ_s. Otherwise we set $t_v = (vs^{-1})^{g_v}$. Letting t denote the element $\sum_{v\in V}^{\perp} t_v v$, we see that

$$\begin{aligned} vx^f &= (vx)^{fv} = (vx)^{g_v^{-1}inn(s)g_v} \\ &= \left[(vs^{-1})\left(vx^{g_v^{-1}}\right)(vs)\right]^{g_v} = inn(t_v)(vx) = vx^{inn(t)} \end{aligned}$$

for all $v \in V$, $x \in Q_s$ and so $f = inn(t) \in G_i$. The proof is complete.

A subgroup $H \subseteq \widehat{G}(R)$ is called an *O-subgroup* if H is an orthogonally complete subset of $End(Q_s)$ and $e^h = e$ for all $e \in B$, $h \in H$.

Remark 8.2.6 *G_f and G_i are O-subgroups of $\widehat{G}(R)$.*

Proof. Let $V \subseteq B$ be a dense orthogonal subset and $g_v \in G_f$, $v \in V$. Then $g_v = \sum_{u\in U_v}^{\perp} g_{v,u}u$. Setting $W = \{vu \mid v \in V,\ u \in U_v,\ uv \neq 0\}$ and $g = \sum_{v\in V}^{\perp} g_v v$ we see that W is a dense orthogonal subset of B and $gw = gvu = g_v vu = g_v uv = g_{v,u}uv = g_{v,u}w$ for all $w = uv \in W$. Letting h_w denote $g_{v,u}$ where $w = vu$, $v \in V$ and $u \in U_v$, we conclude that $g = \sum_{w\in W}^{\perp} h_w w$.

Note that h_w is a Frobenius (anti)automorphism of wQ_s and so $g \in G_f$.

Next we recall that G_i is the group of all X-inner automorphisms of $S = O(R)$. Clearly $e^h = e$ for any $h = inn(s) \in G_i$ and $e \in B$. Now let V be any dense orthogonal subset of B and let $\alpha_v = inn(s_v) \in G_i$, $v \in V$. Setting $s = \sum_{v\in V}^{\perp} s_v v$ and $t = \sum_{v\in V}^{\perp} s_v^{-1} v$, we infer from Remark 3.1.9 that $ts = st = \sum_{v\in V}^{\perp} v = 1$. Furthermore by Proposition 3.1.10 $s, t \in Q_s$. Next we see that $trs = \sum_{v\in V}^{\perp} s_v^{-1} r s_v v \in S$ for all $r \in S$. Finally, letting $g = \sum_{v\in V}^{\perp} inn(s_v)v$, we note that $r^g = \sum_{v\in V}^{\perp} r^{inn(s_v)} v = r^{inn(s)}$ for all $r \in S$. Thus $g = inn(s) \in G_i$.

The following remark is needed in the course of forming the skew group ring $\widehat{U} \propto \widehat{G}$ which will be needed in section 8.3 when we define the "home" for T-identities.

Remark 8.2.7 *Let $f \in \widehat{G}(R)$ and $\mu \in D(R)$. Then $f^{-1}\mu f \in D(R)$. Furthermore if $\mu \in D_i$, then $f^{-1}\mu f \in D_i$ as well.*

Proof. Clearly $f = \alpha h$ for some $\alpha \in G(R)$, $h \in G_f(R)$. We already know that $\alpha^{-1}\mu\alpha$ is a derivation. Hence without loss of generality we may assume that $\alpha = 1$. Let $h = \sum_{v\in V}^{\perp} h_v v$, where $V \subseteq B$ is a dense orthogonal subset and h_v is a Frobenius (anti)automorphism of vQ_s such that $(vS)^{h_v} = vS$, $v \in V$. Recall that $h^{-1} = \sum_{v\in V}^{\perp} h_v^{-1} v$. Since $e\mu = \mu e$ and $eh = he$ for all $e \in B$, we see that

$$h^{-1}\mu h = \left(\sum_{v\in V}{}^{\perp} h_v^{-1} v\right)\mu h = \sum_{v\in V}{}^{\perp} h_v^{-1}\mu h v = \sum_{v\in V}{}^{\perp} (h_v^{-1}\mu h_v) v.$$

Clearly $h_v^{-1}\mu h_v v$ is a derivation of vS for all $v \in V$. Recalling the relation $End(vS) \subseteq End(S)$ we conclude that it is a derivation of S. Setting $\nu = \sum_{v\in V}^{\perp}(h_v^{-1}\mu h_v)v$ we see that $\nu v = h_v^{-1}\mu h_v v$ is a derivation of S for all $v \in V$. Since V is dense subset of B, we infer that ν is a derivation of S. Thus $h^{-1}\mu h = \nu$ is a derivation of S. The proof is complete.

For $f \in \widehat{G}$ the map $\sigma : c \mapsto f^{-1}cf$, $c \in C$, is an automorphism of C. With Remark 8.2.7 in mind we leave it for the reader to check (just as in section 7.1) that the map $c+\mu \mapsto c^{\sigma}+f^{-1}\mu f$ is indeed a σ-semilinear differential C-Lie algebra automorphism of $\widehat{D}$. This leads to an action of $\widehat{G}$ on $\widehat{U}$ and hence to the skew group ring $\widehat{U} \propto \widehat{G}$.

We recall the partial ordering on B which is given as follows: for $e, f \in B$ $e \leq f$ if $e = ef$. Let H be an O-subgroup of $\widehat{G}(R)$. Elements $\alpha, \beta \in \widehat{G}(R)$ are called *completely distinct* on $e \in B$ modulo H, if either $e = 0$ or for every $0 \neq v \leq e$ we have $\alpha v \notin \beta H v$. Using the fact that $vh = hv$ for all $v \in B$, $h \in H$, it is easy to see that α, β are completely distinct on e modulo H if and only if β, α are completely distinct on e modulo H.

Let $A = \{\alpha_i \mid 1 \leq i \leq n\}$ and $e_1, e_2, \ldots, e_n \in B$. Suppose that either $A \subseteq Aut(S)$, or $A \subseteq Antiaut(S)$, and the following conditions are fulfilled:

(a) $e_i e_j = 0$ for all $1 \leq i \neq j \leq n$;

(b) $e_1 + e_2 + \ldots + e_n = 1$;

(c) $e_k^{\alpha_i^{-1}} = e_k^{\alpha_j^{-1}}$ for all $1 \leq i, j, k \leq n$.

Setting $g = \sum_{i=1}^{n} \alpha_i e_i$ we claim that

$$g \in Aut(S) \cup Antiaut(S). \tag{8.5}$$

Indeed, clearly $S = \oplus_{i=1}^{n} Se_i = \oplus_{i=1}^{n} Se_i^{\alpha_1^{-1}}$. By **(c)** we have that $g = \sum_{i=1}^{n} e_i^{\alpha_1^{-1}} \alpha_i$. Now it is clear that g is an (anti)isomorphism of $S = \oplus_{i=1}^{n} Se_i^{\alpha_1^{-1}}$ onto $S = \oplus_{i=1}^{n} Se_i$.

Let $g \in \widehat{G}(R) \subseteq End(Q_s)$. We set

$$e(g) = E(g-1).$$

Then we have

$$((1-e(g))r)^g = (1-e(g))r \quad \text{for all} \quad r \in S.$$

Moreover

$$\text{if } e \in B \text{ and } (er)^g = er \text{ for all } r \in S, \text{ then } e \leq 1 - e(g). \quad (8.6)$$

Lemma 8.2.8 *Let $\alpha, \beta \in \widehat{G}(R)$ and let H be an O-subgroup of $\widehat{G}(R)$. Given any $0 \neq u \in B$ there exist an element $h = h_{\alpha,\beta,u} \in H$ and an idempotent $e = e_{\alpha,\beta,u} \in B$ such that:*

(i) $e(h) \leq e \leq u$;

(ii) $v^{\alpha^{-1}} = v^{\beta^{-1}}$ *for all* $v \leq e$;

(iii) $\beta e = \alpha h e$ *(and hence* $\beta = \alpha h e + \beta(1-e)$*);*

(iv) α *and* β *are completely distinct on* $u - e$ *modulo* H.

Proof. We set $g = \alpha^{-1}\beta$ and $W = \{w \in Bu \mid gw \in Hw\}$. Clearly if $w \in W$, $v \in B$ and $v \leq w$, then $v \in W$ as well. Let U be a maximal orthogonal subset of W. By Remark 3.1.5 $E(U) = E(W)$ and $V = U \cup \{1 - E(U)\}$ is a dense orthogonal subset of B. According to the definition of the set W for every $v \in U$ there exists an element $h_v \in H$ such that $gv = h_v v$. We set $e = E(U)$, $v_0 = 1 - e$, $h_{v_0} = 1$, $h = \sum_{v \in V}^{\perp} h_v v$. One can readily check that $e(h) \leq e \leq u$ and $\beta e = \alpha h e$. Therefore $\beta = \alpha h e + \beta(1-e)$. According to the definition of an O-subgroup $v^h = v$ for all $v \in B$. From $\beta e = \alpha h e$ one obtains $\alpha^{-1}\beta v = hv$ whence $v^{\alpha^{-1}\beta} v = v$ or $v^{\alpha^{-1}\beta} \leq v$ for all $v \leq e$. Likewise from $\beta h^{-1} e = \alpha e$ one obtains $v^{\beta^{-1}\alpha} \leq v$. Thus $v^{\alpha^{-1}} \leq v^{\beta^{-1}} \leq v^{\alpha^{-1}}$ and so $v^{\alpha^{-1}} = v^{\beta^{-1}}$ for all $v \leq e$. Finally if $0 \neq w \leq u - e$ and $\alpha w \in \beta H w$, then $\alpha w = \beta f w$ for some $f \in H$. Since $fw = wf$, we conclude that $f^{-1}w = \alpha^{-1}\beta w$ and hence $w \in W$. Recalling that $e \leq u$ we see that $e(u - e) = 0$. Therefore $ew = 0$ and so $E(U)w = 0$. It follows that $Uw = 0$, a contradiction to the maximality of U. Thus α and β are completely distinct on $u - e$ modulo H and the proof is complete.

Proposition 8.2.9 *Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \widehat{G}(R)$ and H an O-subgroup of $\widehat{G}(R)$. We set $\alpha_0 = 1$. Then there exist idempotents*

$u_{ki} \in B$ and elements $h_{ki} \in H$, $k = 1, 2, \ldots, n$, $i = 0, 1, \ldots, k$ such that:

(i) *$u_{k0}, \ldots, u_{kk}$ are pairwise orthogonal idempotents whose sum is equal to 1 for all $k = 1, 2, \ldots, n$;*

(ii) *$\alpha_k = \sum_{i=0}^{k} \alpha_i h_{ki} u_{ki}$ for all $k = 1, 2, \ldots, n$;*

(iii) *α_k and α_j are completely distinct on $u_{jj}(1 - \sum_{i=0}^{j} u_{ki})$ modulo H for all $k = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, k-1$;*

(iv) *α_k and α_j are completely distinct on $u_{kk}u_{jj}$ modulo H for all $k \neq j$;*

(v) *$h_{kk} = 1$ for all $k = 1, 2, \ldots, n$;*

(vi) *$e(h_{ki}) \leq u_{ki} \leq u_{ii}$ for all $k = 1, \ldots, n$, $i = 1, \ldots, k-1$;*

(vii) *$u_{k0} \geq 1 - e(\alpha_k)$ for all $k = 1, 2, \ldots, n$;*

(viii) *$v^{\alpha_k^{-1}} = v^{\alpha_i^{-1}}$ for all $k = 1, 2, \ldots, n$, $i = 0, 1, \ldots, k-1$ and $v \leq u_{ki}$.*

Proof. The lower triangular array of idempotents $u_{kj} \in B$ (along with the accompanying elements $h_{kj} \in H$) is constructed column by column as follows. For column 0 we let $u_{00} = 1$ play the role of u in Lemma 8.2.8 and set $u_{k0} = e_{1,\alpha_k,1}$ and $h_{k0} = h_{1,\alpha_k,1}$. Now assume columns $0, 1, \ldots, t$ have been constructed and we proceed to construct column $t+1$. We set

$$u_{t+1,t+1} = 1 - \sum_{i=0}^{t} u_{t+1,i}, \quad h_{t+1,t+1} = 1 \tag{8.7}$$

For each $k > t+1$ we let

$$w_{k,t+1} = u_{t+1,t+1}\left(1 - \sum_{i=0}^{t} u_{k,i}\right) \tag{8.8}$$

play the role of u in Lemma 8.2.8 and set

$$u_{k,t+1} = e_{\alpha_{t+1},\alpha_k,w_{k,t+1}} \tag{8.9}$$

$$h_{k,t+1} = h_{\alpha_{t+1},\alpha_k,w_{k,t+1}} \tag{8.10}$$

By (8.7) $\sum_{j=0}^{k} u_{kj} = 1$. By (8.9) $u_{kj} \leq w_{kj} \leq 1 - \sum_{i=0}^{j-1} u_{ki}$. The sum $\sum_{i=0}^{k} u_{ki}$ is therefore direct and so **(i)** is proved. By the definition of $e(\alpha_k)$ we have $(\alpha_k - 1)(1 - e(\alpha_k)) = 0$, i.e., $\alpha_k(1 - e(\alpha_k)) = 1 \cdot (1 - e(\alpha_k))$, $k = 1, 2, \ldots, n$. Since $1 \in H$ this puts $1 - e(\alpha_k) \leq u_{k0}$, $k = 1, 2, \ldots, n$ and so **(vii)** is proved. By (8.7) $h_{kk} = 1$ by definition, which establishes **(v)**. An appropriate application of Lemma 8.2.8 gives $e(h_{ki}) \leq w_{ki}$ (see (8.10). It follows from (8.8) that $w_{ki} \leq u_{ki}$ and so $e(h_{ki}) \leq u_{ki}$. By (8.8) and (8.9) we have $u_{ki} \leq u_{ii}$. Thus **(vi)** is proved. By Lemma 8.2.8**(ii)**, **(viii)** is clear. Since

$$\begin{aligned}
\alpha_k &= \alpha_k(u_{k0} + u_{k1} + \ldots + u_{kk}) \\
&= \alpha_k u_{k0} + \alpha_k u_{k1} + \ldots + \alpha_k u_{kk} \\
&= \alpha_0 h_{k0} u_{k0} + \alpha_1 h_{k1} u_{k1} + \ldots + \alpha_k h_{kk} u_{kk}
\end{aligned}$$

(using Lemma 8.2.8**(iii)**) we have thereby proved **(ii)**. From Lemma 8.2.8**(iv)** we know that α_k, α_j, $k > j$, are completely distinct on

$$w_{kj} - u_{kj} = u_{jj}\left(1 - \sum_{i=0}^{j-1} u_{ki}\right) - u_{kj} = u_{jj}\left(1 - \sum_{i=0}^{j} u_{ki}\right),$$

which proves **(iii)**. In particular, since $u_{kk} \leq 1 - \sum_{i=0}^{j} u_{ki}$, we see that α_k, α_j are completely distinct on $u_{jj}u_{kk}$. Thus **(iv)** is shown and the proof is complete.

Lemma 8.2.10 *Let $\alpha \in \widehat{G}(R)$. Then:*

(i) The restriction $\alpha|_B$ of α on B is an automorphism of B; In particular $M^\alpha \in Spec(B)$ for all $M \in Spec(B)$;

(ii) Given $M \in Spec(B)$, the mapping $\alpha_M : Q_s/MQ_s \to Q_s/M^\alpha Q_s$ defined by the rule $x + MQ_s \mapsto x^\alpha + M^\alpha Q_s$, $x \in Q_s$, is either an isomorphism (if $u_1(g) \notin M$) or an antiisomorphism (if $u_2(g) \notin M$).

Proof. **(i)** Since $\widehat{G} = GG_f$, $\alpha = gh$ for some $g \in G$, $h \in G_f$. By Corollary 8.2.3 we have $e^h = e$ for all $e \in B$. Therefore $e^\alpha = e^g$ for all $e \in B$ and so $\alpha|_B = g|_B$ is an automorphism of B.

(ii) It follows from Remark 8.2.2 that there exist two orthogonal idempotents $u_1 = u_1(g), u_2 = u_2(g) \in B$ such that $u_1 + u_2 = 1$, $hu_1 \in Aut(u_1S)$ and $hu_2 \in Antiaut(u_2S)$. If $u_1 \in M^\alpha$, then $(x + MQ_s)^{\alpha_M} = x^{ghu_2} + M^\alpha Q_s$. Otherwise $(x + MQ_s)^{\alpha_M} = x^{ghu_1} + M^\alpha Q_s$. Thus in the first case α_M is an antiisomorphism while in the second case it is an isomorphism. The proof is complete.

The following general result may be of independent interest since it gives a decomposition of B relative to an automorphism α.

Lemma 8.2.11 *Let α be any automorphism of the Boolean ring $B \subseteq C$. Then there exists pairwise orthogonal idempotents $e_{\alpha,0}, e_{\alpha,1}, e_{\alpha,2}, e_{\alpha,3} \in B$ such that:*

(i) $e_{\alpha,0} + e_{\alpha,1} + e_{\alpha,2} + e_{\alpha,3} = 1$;

(ii) $e_{\alpha,1}^\alpha \leq e_{\alpha,2}$, $e_{\alpha,2}^\alpha = e_{\alpha,3}$ and $e_{\alpha,3}^\alpha = e_{\alpha,1} + e_{\alpha,2}e_{\alpha,3}^\alpha$;

(iii) If $e \leq e_{\alpha,0}$, then $e^\alpha = e$.

Proof. Let $A \subseteq B$. We note that $r_B(A) = r_C(A) \cap B = (1 - E(A))B$. Next we claim that

$$E(A^\alpha) = E(A)^\alpha. \tag{8.11}$$

Indeed, we have

$$(1 - E(A^\alpha))B = r_B(A^\alpha) = r_B(A)^\alpha = (1 - E(A)^\alpha)B$$

which proves our claim. Next we claim that

$$\text{if} \quad AA^\alpha = 0, \text{ then} \quad E(A)E(A)^\alpha = 0. \tag{8.12}$$

Indeed, since $ACA^\alpha = 0$, from Lemma 2.3.10 (with C instead of R) we see that $E(A)E(A^\alpha) = 0$. Now by (8.11) we have $E(A)E(A)^\alpha = 0$ and our claim is established.

Given $v \in B$ we set $U(v) = \{u \in B \mid uu^\alpha = 0 = uv\}$. Consider any chain $A \subseteq U(v)$ (i.e., a subset $A \subseteq U(v)$ such that for all $a, b \in A$ either $a \leq b$, or $b \leq a$). We claim that $E(A) \subseteq U(v)$. Indeed, let $a, b \in A$. Then either $a \leq b$, or $b \leq a$. In the first case we have

$$a^\alpha b = (ab)^\alpha b = a^\alpha(b^\alpha b) = 0.$$

In the second case we see that

$$a^\alpha b = a^\alpha(ab) = (a^\alpha a)b = 0.$$

Therefore $AA^\alpha = 0$ and so $E(A)E(A)^\alpha = 0$ by (8.12). Finally since $Av = 0$, $v \in r_C(A) = (1 - E(A))C$ and hence $vE(A) = 0$. Thus $E(A) \in U(v)$. Since $E(A)a = a$ for all $a \in A$, we see that every chain in $U(v)$ has an upper bound. Therefore Zorn's Lemma is applicable and so

$$U(v) \quad \text{contains maximal elements.} \tag{8.13}$$

Clearly α^{-1} preserves the partial ordering $\leq$ and $U(v)^{\alpha^{-1}} = U(v^{\alpha^{-1}})$. Hence if a is a maximal element of $U(v)$, then

$$a^{\alpha^{-1}} \text{ is a maximal element of } U(v^{\alpha^{-1}}) \tag{8.14}$$

Let $v \in B$ and let a be a maximal element in $U(0)$. We now show

$$\text{if } vv^\alpha = 0 = v(a + a^\alpha), \text{ then } v^\alpha a = v^\alpha. \tag{8.15}$$

To this end we set $w = v(1 - a^{\alpha^{-1}})$ and note that $vw = w$. We claim that

$$ww^\alpha = wa = wa^\alpha = w^\alpha a = 0. \tag{8.16}$$

Indeed, since $vv^\alpha = 0$, $ww^\alpha = 0$ as well. As $aa^\alpha = 0$ and $v(a + a^\alpha) = 0$, we infer that $va = 0 = va^\alpha$. Recalling that

$w = vw$, we conclude that $wa = wa^{\alpha} = 0$. Finally since $w^{\alpha} = v^{\alpha}(1-a)$, we see that $w^{\alpha}a = 0$ which proves our claim. It follows from (8.16) that $(w+a)(w+a)^{\alpha} = 0$, $(w+a)^2 = w+a$ and so $w + a \in U(0)$. Since $w + a \geq a$ and a is a maximal element in $U(0)$, we conclude that $w = 0$ and hence $v = va^{\alpha^{-1}}$. Applying α we see that $v^{\alpha} = v^{\alpha}a$.

Let e be a maximal element in $U(0)$ and let u be a maximal element in $U(e+e^{\alpha})$. Then by (8.15) we have that

$$u^{\alpha}e = u^{\alpha}. \tag{8.17}$$

Let $v \in B$. We claim that

$$\text{if } v(u+e+e^{\alpha}) = 0, \text{ then } v^{\alpha}v = v^{\alpha}. \tag{8.18}$$

Indeed, suppose that $v^{\alpha}v \neq v^{\alpha}$. Then $vv^{\alpha^{-1}} \neq v$ and so $w = v(1 - v^{\alpha^{-1}}) \neq 0$. We show that

$$w(e+e^{\alpha}) = wu = wu^{\alpha} = ww^{\alpha} = uw^{\alpha} = 0. \tag{8.19}$$

Indeed, since u, e and e^{α} are pairwise orthogonal, we infer from $v(u+e+e^{\alpha}) = 0$, that $vu = ve = ve^{\alpha} = 0$. Recalling that $vw = w$, we conclude that $wu = we = we^{\alpha} = 0$ and so $w(e+e^{\alpha}) = 0$. From (8.17) and $we = 0$ we infer that $wu^{\alpha} = 0$. Since $w^{\alpha} = v^{\alpha}(1-v)$ and $wv = w$, $ww^{\alpha} = 0$. Finally since $w(e+e^{\alpha}) = 0 = ww^{\alpha}$, we have by (8.15) that $w^{\alpha}e = w^{\alpha}$. Now from $ue = 0$ we obtain that $uw^{\alpha} = 0$. Thus (8.19) is proved. From (8.19) we see that $w+u$ is an idempotent such that $(w+u)(e+e^{\alpha}) = 0 = (w+u)(w+u)^{\alpha}$. Hence $w+u \in U(e+e^{\alpha})$ which contradicts the maximality of u. Thus $v^{\alpha}v = v^{\alpha}$ and our claim is proved. Next we claim that

$$\text{if } v(u+e+e^{\alpha}) = 0, \text{ then } v^{\alpha} = v. \tag{8.20}$$

Indeed, let $w = v(1-v^{\alpha})$. Then clearly $w(u+e+e^{\alpha}) = 0$. Now from (8.18) (with w instead of v) we see that $0 = ww^{\alpha} = w^{\alpha}$ and so $w = 0$. Hence $v = vv^\alpha$. By (8.18) we have $vv^\alpha = v^\alpha$ and so $v = v^\alpha$ which proves our claim. In particular $(1-u-e-e^\alpha)^\alpha = 1-u-e-e^\alpha$. Therefore $(u+e+e^\alpha)^\alpha = u+e+e^\alpha$ and so $(u+e+e^\alpha)^{\alpha^{-1}} = u+e+e^\alpha$. It follows that $u^{\alpha^{-1}} \leq u+e+e^\alpha$ and hence $u^{\alpha^{-1}} = u_1+u_2+u_3$ where $u_1 \leq u$, $u_2 \leq e$ and $u_3 \leq e^\alpha$. We have $u = u_1^\alpha+u_2^\alpha+u_3^\alpha$. Since $u_1 \leq u$, $u_1^\alpha \leq u^\alpha$. On the other hand $uu^\alpha = 0$ and we conclude from $u = u_1^\alpha+u_2^\alpha+u_3^\alpha$ that $u_1 = 0$. As $u_2 \leq e$, $u_2^\alpha \leq e^\alpha$. Now from $ue^\alpha = 0$ we infer that $u_2 = 0$. Hence $u^{\alpha^{-1}} = u_3 \leq e^\alpha$ and so $u \leq e^{\alpha^2}$. Further $e^{\alpha^2}e^\alpha = (e^\alpha e)^\alpha = 0$. Since $e^\alpha \leq u+e+e^\alpha$ and $(u+e+e^\alpha)^\alpha = u+e+e^\alpha$, we infer that $e^{\alpha^2} \leq u+e'$ where $e' \leq e$. Recalling that $ue = 0$ we see that $e' = ee^{\alpha^2}$. Now setting $e_{\alpha,0} = 1-u-e-e^\alpha$, $e_{\alpha,1} = u$, $e_{\alpha,2} = e$ and $e_{\alpha,3} = e^\alpha$ and recalling that $e_{\alpha,1}^\alpha \leq e_{\alpha,2}$ by (8.17) we complete the proof.

Corollary 8.2.12 *Let α be any automorphism of the Boolean ring $B \subseteq C$ and let idempotents $e_{\alpha,0}, e_{\alpha,1}, e_{\alpha,2}, e_{\alpha,3} \in B$ be as in Lemma 8.2.11. Further let $M \in Spec(B)$. Then $M^\alpha = M$ if and only if $e_{\alpha,0} \notin M$.*

Proof. We set $e_i = e_{\alpha,i}$, $i = 0,1,2,3$. Let $M^\alpha = M$. Then $M^{\alpha^{-1}} = M$ as well. Since $e_i^\alpha e_i = 0$ for $i = 1,2,3$, we obtain that either $e_i \in M$ or $e_i^\alpha \in M$. In the last case $e_i \in M^{\alpha^{-1}} = M$. Therefore $e_i \in M$ for $i = 1,2,3$ and so $e_0 = 1-e_1-e_2-e_3 \notin M$.

Next let $e_0 \notin M$. Recall that the addition $\oplus$ of the Boolean ring B is given by the rule $u \oplus v = u+v-2uv$, $u, v \in B$. Now suppose that $M^\alpha \neq M$. Since M is a maximal ideal of the Boolean ring B, we infer that $M \oplus M^\alpha = B$. It follows that $u+v-2uv = e_0$ for some $u \in M$, $v \in M^\alpha$. Setting $x = u(1-v)$ and $y = v(1-u)$, we see that

$$xy = 0,\ x+y = e_0,\ x \in M \quad \text{and} \quad y \in M^\alpha.$$

It follows that $y \leq e_0$. By Lemma 8.2.11(**iii**) we have $y^\alpha = y$ and so $y = y^{\alpha^{-1}} \in M$. Therefore $e_0 = x+y \in M$ which contradicts the relation $e_0 \notin M$. Thus $M^\alpha = M$ and the proof is complete.

Given $\alpha \in \widehat{G}(R)$ and $P \in Spec(B)$, recall that the map $\alpha_P : S/PS \to S/P^\alpha S$ defined by the rule $x + PS \mapsto x^\alpha + P^\alpha S$, $x \in S$, is either an isomorphism or an antiisomorphism of rings (see Lemma 8.2.10). The next two results lead up to Corollary 8.2.15, which makes possible an important link between completely distinct elements modulo G_i and $G_0(\overline{S})$ in certain situations.

Lemma 8.2.13 *Let $\alpha \in \widehat{G}$ and $P \in Spec(B)$. Suppose that $P^\alpha = P$ and $\alpha_P \in G_i(S/PS)$. Then there exist elements b, a_1, a_2 $\in S$ such that:*
(i) $E(a_1) = E(a_2) = E(b) \notin P$;
(ii) $bx^\alpha b = a_1 x a_2$ for all $x \in S$;
(iii) $\alpha E(b) \in Aut(E(b)S)$;

Proof. Let $\phi_P : S \to \overline{S} = S/PS$ be the canonical ring surjection and let $e_i = e_{\alpha,i}$, $i = 0, 1, 2, 3$ (see Lemma 8.2.11). We have $\alpha_P = inn(s)$ for some $s \in Q_s(\overline{S})$. Obviously $Is^{-1}, sI \subseteq \overline{S}$ for some nonzero ideal of $\overline{S}$. Pick any $0 \neq \overline{b} \in I$ and set $\overline{a}_1 = \overline{b}s^{-1}$, $\overline{a}_2 = s\overline{b}$. Since s is an invertible element of $Q_s(\overline{S})$, $\overline{a}_1 \neq 0 \neq \overline{a}_2$. We note that

$$\overline{b}x^{\alpha_P}\overline{b} - \overline{a}_1 x \overline{a}_2 = 0 \quad \text{for all} \quad x \in \overline{S}. \tag{8.21}$$

Clearly $\overline{b} = \phi_P(b')$, $\overline{a}_1 = \phi_P(a_1')$ and $\overline{a}_2 = \phi_P(a_2')$ for some $b, a_1', a_2' \in S$. It follows from Corollary 3.2.4 that

$$E(b'), E(a_1'), E(a_2') \notin P.$$

Since $P^\alpha = P$, we conclude from Corollary 8.2.12 that $e_0 \notin P$. Hence $(1 - e_0)x \in PS$ for all $x \in S$ and so $\phi_P(e_0 x) = \phi_P(x)$. Therefore without loss of generality we can assume that $e_0 b' = b'$, $e_0 a_1' = a_1'$ and $e_0 a_2' = a_2'$. Further it follows from Lemma 8.2.10

that $u_1 = u_1(\alpha) \notin P$ and so we can assume that $u_1 b' = b'$, $u_1 a_1' = a_1'$ and $u_1 a_2' = a_2'$. Setting $H = \{b'x^\alpha b' - a_1' x a_2' \mid x \in S\}$, we claim that H is an orthogonally complete subset of S. Indeed, let V be a dense orthogonal subset of B and $\{h_v = b'x_v^\alpha b' - a_1' x_v a_2' \mid v \in V\}$. By Lemma 8.2.11(**iii**) we have

$$v^\alpha e_0 = v^\alpha e_0^\alpha = (ve_0)^\alpha = ve_0 \quad \text{for all} \quad v \in V.$$

Letting $x = \sum_{v\in V}^{\perp} x_v v$ and recalling that $b'e_0 = b'$, we see that

$$\begin{aligned} \sum_{v\in V}{}^{\perp}(b'x_v^\alpha b' - a_1' x_v a_2')v &= \sum_{v\in V}{}^{\perp}(b'x_v^\alpha b')(e_0 v) - a_1' x a_2' \\ &= b'\left(\sum_{v\in V}{}^{\perp} x_v e_0 v\right)^\alpha b' - a_1' x a_2' \\ &= b'\left[\left(\sum_{v\in V}{}^{\perp} x_v v\right) e_0\right]^\alpha b' - a_1' x a_2' \\ &= b'\left(\sum_{v\in V}{}^{\perp} x_v v\right)^\alpha (e_0 b') - a_1' x a_2' \\ &= b'x^\alpha b' - a_1' x a_2' \in H \end{aligned}$$

and hence H is orthogonally complete.

It follows from (8.21) that $\phi_P(H) = 0$ and so $eH = 0$ for some $e \in B \setminus P$ (see Corollary 3.2.4(**iii**)). Setting

$$\begin{aligned} b &= E(b')E(a_1')E(a_2')eb', \\ a_1 &= E(b')E(a_1')E(a_2')ea_1' \quad \text{and} \\ a_2 &= E(b')E(a_1')E(a_2')ea_2', \end{aligned}$$

we see that $bx^\alpha b - a_1 x a_2 = 0$ for all $x \in S$. Further by Theorem 2.3.9(**ii**) we have that

$$E(b) = E(a_1) = E(a_2) = E(b')E(a_1')E(a_2')e \notin P.$$

Since $u_1 b' = b'$, we see that $u_1 b = b$ and so $u_1 \geq E(b)$. It is now clear that $\alpha E(b) \in Aut(E(b)S)$. The proof is thereby complete.

Given $\alpha \in \widehat{G}$, we set

$$M_\alpha = \{s \in Q \mid rs = sr^\alpha \quad \text{for all} \quad r \in S\}.$$

Lemma 8.2.14 *Let $\alpha \in \widehat{G}$. Suppose that there exist $b, a_1, a_2 \in S$ such that $E(b) = E(a_1) = E(a_2) = e \neq 0$, $\alpha e \in Aut(eS)$ and*

$$bx^\alpha b - a_1 x a_2 = 0 \quad \textit{for all} \quad x \in S. \tag{8.22}$$

Then there exists an element $s \in M_\alpha$ such that $E(s) = e$, $a_1 s = b$ and $a_2 = sb$.

Proof. Replacing S by eS, we may assume that $e = 1$ (whence $E(b) = E(a_1) = E(a_2) = 1$) and $\alpha \in Aut(S)$. Suppose that $a_2 \notin M_\alpha b$. Then a_2 is left independent of b re 1, α (see Section 2.5). By Theorem 2.3.3 there exists $\beta = \sum r_i \otimes s_i \in S^\circ \otimes_C S$ such that $a_2 \cdot \beta \neq 0$ but $b \cdot \beta^\alpha = 0$. Substituting xr_i for x in (8.22) and multiplying by s_i from the right, we obtain

$$bx^\alpha r_i^\alpha b s_i - a_1 x r_i a_2 s_i = 0$$

and so

$$bx^\alpha (b \cdot \beta^\alpha) - a_1 x (a_2 \cdot \beta) = 0$$

for all $x \in S$. Since $b \cdot \beta^\alpha = 0$, we see that $a_1 x (a_2 \cdot \beta) = 0$ for all $x \in S$. As $E(a_1) = 1$, it follows from Lemma 2.3.10 that $0 = E(a_1)(a_2 \cdot \beta) = a_2 \cdot \beta$ in contradiction to the choice of β. Therefore $a_2 \in M_\alpha b$ and so $a_2 = sb$ for some $s \in M_\alpha$. Clearly $E(s) \geq E(a_2) = 1$. Hence $E(s) = 1$. By Proposition 3.1.12 we have that s is an invertible element of Q_s and so $\alpha = inn(s)$. Now we have $(bs^{-1} - a_1)xsb = bs^{-1}xsb - a_1 xsb = 0$ for all $x \in S$. Applying Lemma 2.3.10, we obtain that $E(sb)(bs^{-1} - a_1) = 0$. Since $E(sb) = E(b) = 1$, it follows that $bs^{-1} = a_1$ and so $b = a_1 s$. The proof is complete.

The following result will be useful in section 8.4.

Corollary 8.2.15 *Let $\alpha \in \widehat{G}(R)$ and $P \in Spec(B)$. Suppose that $P^\alpha = P$. Then $\phi_P(M_\alpha) = M_{\alpha_P}$ and $\alpha e \in G_i e$ for some $e \in B \setminus M$.*

Proof. Obviously $\phi_P(M_\alpha) \subseteq M_{\alpha_P}$. Now suppose that $M_{\alpha_P} \neq 0$. It follows from Lemma 8.2.13 and Lemma 8.2.14 that there exists an element $s \in M_\alpha$ such that $E(s) \notin P$ and $\alpha E(s) \in Aut(SE(s))$. Hence $\phi_P(s) \neq 0$ by Corollary 3.2.4. From Proposition 3.1.12 we know that M_{α_P} is a cyclic $\phi_P(C)$-module. Since $\phi_P(C)$ is a field and $0 \neq \phi_P(s) \in M_{\alpha_P}$, we conclude that $\phi_P(M_\alpha) = M_{\alpha_P}$. By Proposition 3.1.12 we have that s is an invertible element of $Q_s E(s)$ and so $\alpha E(s) = inn(s) \in G_i(Q_s E(s))$. Therefore $t = s + 1 - E(s)$ is an invertible element of Q_s and $\alpha E(s) = inn(t)E(s)$. The proof is thereby complete.

Our final result of this section is important because it makes possible a link between completely distinct elements modulo G_f and representatives of $G(\overline{S})$ modulo $G_f(\overline{S})$ in certain situations.

Lemma 8.2.16 *Let $\alpha \in \widehat{G}(R)$ and $P \in Spec(B)$. Suppose that $P^\alpha = P$ and α_P is a Frobenius (anti)automorphism of $\overline{S} = S/PS$. Then there exists an idempotent $e \in B \setminus P$ such that $\alpha e \in G_f e$.*

Proof. We set

$$p = \begin{cases} char(\overline{C}) & \text{if } char(\overline{C}) > 0, \\ 1 & \text{if } char(\overline{C}) = 0. \end{cases}$$

and $e_i = e_{i,\alpha}$, $i = 0, 1, 2, 3$ (see Lemma 8.2.11). By Corollary 8.2.12 we have that $e_0 \notin P$. Recall that $v^\alpha = v$ for all $v \leq e_0$ (see Lemma 8.2.11). It follows from our assumptions that there exists a natural number n such that for all $x \in \overline{C}$ either $\alpha_P(x) = x^{p^n}$ or $(\alpha_P(x))^{p^n} = x$. Accordingly we set H to be equal to either $\{\alpha(x) - x^{p^n} \mid x \in e_0 C\}$ or $\{\alpha(x)^{p^n} - x \mid x \in e_0 C\}$. Since $v^\alpha = v$ for all $v \leq e_0$, one can easily check that H is an orthogonally complete subset of S. Clearly $\phi_P(H) = 0$ and so $uH = 0$ for some $u \in B \setminus P$ (see Corollary 3.2.4). Next we set T to be equal $\{\alpha(x)\alpha(y) - \alpha(xy) \mid x, y \in e_0S\}$ if α_P is an automorphism and $\{\alpha(y)\alpha(x) - \alpha(xy) \mid x, y \in e_0S\}$ if α_P is an antiautomorphism of $\overline{S}$. Again one can easily check that T is an orthogonally complete subset of S and $\phi_P(T) = 0$. Therefore $vT = 0$ for some $v \in B \setminus P$. Setting $e = e_0uv$, we see that for all $x \in eC$ either

$$\alpha(x) = \alpha(ex) = e\alpha(x) = ex^{p^n} = x^{p^n}$$

or

$$(\alpha(x))^{p^n} = (\alpha(ex))^{p^n} = e(\alpha(x))^{p^n} = ex = x$$

and hence α is a Frobenius (anti)automorphism of e_0S. We define $\beta : S \to S$ by the rule $\beta(x) = \alpha(ex) + (1 - e)x$ for all $x \in S$. Clearly $\beta \in G_f$ and $\alpha e = \beta e$. The proof is complete.

8.3 The Home of $\widehat{T}$-identities

Let R be a semiprime ring, $S = O(R)$ its orthogonal completion, $Q_s = Q_s(S)$, and $Q = Q_{mr}(R) = Q_{mr}(S)$. Our first task is to define the notion of $\widehat{T}$-identity, and it turns out that this may be done in the way it was done for prime rings in Chapter 7. We have already mentioned in section 8.2 (see Remark 8.2.7 and the comments following it) that the skew group ring $\widehat{T} = \widehat{T}(R) = \widehat{U} \propto \widehat{G}$ can be formed. Proceeding in an analogous fashion to section 7.1 one can readily show that $\widehat{T}$ is a C-ring and that there exists a C-ring homomorphism $\gamma : \widehat{T} \to End(Q_s)$ defined in a natural way. Let V be a free right C-module with infinite basis X. We then form the right C-module $V \otimes_C \widehat{T}$ with scalar multiplication given by

$$(v \otimes t)c = v \otimes tc, \quad v \in V,\ c \in C$$

(since C is a commutative ring, the tensor product of right C-modules is a right C-module as well). Further we form

$$\widehat{\mathcal{S}}_m = Q \coprod_C C\{V \otimes_C \widehat{T}\}$$

which we shall call *the maximal setting of* R (here we are emulating section 7.8 but the reader may feel more comfortable using Q_s instead of Q and simply forming the setting $\widehat{\mathcal{S}}$ with reference to section 7.1).

A substitution process compatible with $\widehat{\mathcal{S}}_m$ is described analogously to that in section 7.8 as follows. Let P be a C-algebra with 1 such that

(i) $P \supseteq Q$;

(ii) $P \supseteq K$, K a C-subalgebra of P;

(iii) There is a C-ring map $\sigma : \widehat{T} \to End_\Phi(K)$.

Let $\psi : V \to K$ be any C-module map. Then (as in section 7.1) it can be shown that there is a unique C-algebra map $\widetilde{\psi} : \widehat{\mathcal{S}}_m \to P$ given by $q \mapsto q$, $q \in Q$, and $v \otimes t \mapsto \psi(v)^{\sigma(t)}$, $v \in V$, $t \in \widehat{T}$. Such a map will be called *a* $\widehat{T}'$*-substitution determined by* ψ *relatively to* σ . Now let $P = Q$, $K = Q_s$, and $\sigma = \gamma$. Given a nonzero ideal I of R, an element g of $\widehat{\mathcal{S}}_m$ is called *a* $\widehat{T}'$*-identity on* I if g is mapped to 0 under all $\widehat{T}'$-substitutions $\widetilde{\psi}$ for which $\psi(X) \subseteq I$. Further a $\widehat{T}'$-identity $g \in \widehat{\mathcal{S}}_m$ on an ideal I of R is said to be *strict* if $r_C(g) \subseteq r_C(I)$.

We define the set $\widehat{I}_0$ of trivial $\widehat{T}'$-identities of R to be the ideal of $\widehat{\mathcal{S}}_m$ generated by all elements of the following two forms:

(C_1') $v \otimes t\mu - [a, v \otimes t]$, $\mu = ad(a) \in D_i$

(C_2') $v \otimes th - s^{-1}(v \otimes t)s$, $h = inn(s) \in G_i$

where $v \in V$, $t \in \widehat{T}$.

In contrast to the situation for prime rings in Chapter 7 $\widehat{U}$ has no PBW-basis and Q and $\widehat{T}$ need not be free C-modules. As a result the notion of *degree* and *height* for elements of $\widehat{\mathcal{S}}_m$ as well as the notion of (Frobenius) reduced element of $\widehat{\mathcal{S}}_m$ cannot be defined in the usual way. Fortunately weaker definitions for these notions can be given which will suffice for our purposes. We now proceed to present these in a rigorous fashion and then, having done so, we will feel free to take some liberty with the notation.

In these last two sections we shall be interested in arbitrary, reduced, and G_f-reduced elements of $\widehat{\mathcal{S}}_m$. It is therefore appropriate to consider respectively the following types of finite sequences:

$$\begin{aligned} \tau &= ((x_1, \Delta_1, \alpha_1), (x_2, \Delta_2, \alpha_2), \ldots, (x_n, \Delta_n, \alpha_n)) && (8.23)\\ \tau &= ((x_1, \Delta_1, \alpha_1, v_1), \ldots, (x_n, \Delta_n, \alpha_n, v_n)) && (8.24)\\ \tau &= ((x_1, \Delta_1, \alpha_1, h_1, v_1), \ldots, (x_n, \Delta_n, \alpha_n, h_n, v_n)) && (8.25)\end{aligned}$$

where $x_i \in X$, $\Delta_i \in \widehat{U}$, $\alpha_i \in \widehat{G}$, $h_i \in G_f$, $v_i \in B$. In (8.24) and (8.25) the Δ_i's will be appropriate correct monomials, and the α_i's and h_i's will be appropriate completely independent elements. We then define deg(τ) and $ht(\tau)$ in the obvious way, i.e., deg$(\tau) = n$ and $ht(\tau) = n$ minus the number of distinct x_i's appearing in τ. Any finite sum S_τ of elements of the form

$$a_0 x_1^{\Delta_1 \alpha_1 (h_1 v_1)} a_1 \ldots x_n^{\Delta_n \alpha_n (h_n v_n)} a_n$$

will be called *a generalized monomial determined by* τ or simply *a* τ*-monomial* . For $S_\tau \neq 0$ we define deg$(S_\tau) =$ deg(τ) and $ht(S_\tau) = ht(\tau)$. Next let $\rho = \{S_{\tau_1}, S_{\tau_2}, \ldots, S_{\tau_m}\}$ be a finite subset of distinct τ-monomials and let $f \in \widehat{\mathcal{S}}_m$ be such that $f = f_\rho = \sum_{i=1}^m S_{\tau_i}$. We shall call ρ *a support of* f and refer to f_ρ as *the representation of* f *with respect to* ρ . Then the ρ-deg $f =$ max$\{$deg$(S_\tau) \mid 0 \neq S_\tau \in \rho\}$ and the ρ-$ht(f) =$ max$\{ht(S_\tau) \mid 0 \neq S_\tau \in \rho\}$. It will also be useful to define $M_\rho(f) = |\rho| = m$. Since the same element f may have many different supports, it will of course have many different ρ-degrees and ρ-heights attached to it. When the context is clear (i.e., when a particular support has been determined) we will often simply write f, deg(f), $ht(f)$, $M(f)$ in place of, respectively, f_ρ, ρ-deg(f), ρ-$ht(f)$, $M_\rho(f)$.

An element $g \in \widehat{\mathcal{S}}_m$ is called *reduced* if there is a strongly independent subset $\mathcal{M}$ of $D(R)$ such that $g = \sum S_\tau$, τ of the form (8.24), where

(R_1) Every Δ_j is a correct monomial in $\mathcal{M}$;

(R_2) $0 \neq v_t \leq E(\Delta_j)^{\alpha_k}$ for each $x^{\Delta_j \alpha_k v_t}$ involved in g;

(R_3) α_{k_1}, α_{k_2} are completely distinct on $v_{t_1}v_{t_2}$ modulo G_i for all $x^{\Delta_{j_1}\alpha_{k_1}v_{t_1}}$ and $x^{\Delta_{j_2}\alpha_{k_2}v_{t_2}}$ involved in g such that $k_1 \neq k_2$.

Similarly, an element $g \in \widehat{\mathcal{S}}_m$ is called G_f*-reduced* if there is a strongly independent subset $\mathcal{M}$ of $D(R)$ such that $g = \sum S_\tau$, τ of the form (8.25), where

(GR_1) Every Δ_j is a correct monomial in $\mathcal{M}$;

(GR_2) $v_t \leq E(\Delta_j)^{\alpha_k}$ for all $x^{\Delta_j \alpha_k h_l v_t}$ involved in g;

(GR_3) α_{k_1} and α_{k_2} are completely distinct on $v_{t_1}v_{t_2}$ modulo G_f for all $x^{\Delta_{j_1}\alpha_{k_1}h_{l_1}v_{t_1}}$ and $x^{\Delta_{j_2}\alpha_{k_2}h_{l_2}v_{t_2}}$ involved in g such that $k_1 \neq k_2$;

(GR_4) h_{l_1} and h_{l_2} are completely distinct on $v_{t_1}v_{t_2}$ modulo G_i for all $x^{\Delta_{j_1}\alpha_{k_1}h_{l_1}v_{t_1}}$ and $x^{\Delta_{j_2}\alpha_{k_2}h_{l_2}v_{t_2}}$ involved in g such that $l_1 \neq l_2$.

Since $G_i \subseteq G_f$, we conclude from (GR_2) and (GR_3) that $\alpha_{k_1}f_{l_1}$ and $\alpha_{k_2}f_{l_2}$ are completely distinct on $v_{t_1}v_{t_2}$ modulo G_i for all $x^{\Delta_{j_1}\alpha_{k_1}h_{l_1}v_{t_1}}$ and $x^{\Delta_{j_2}\alpha_{k_2}h_{l_2}v_{t_2}}$ involved in g such that $(k_1, l_1) \neq (k_2, l_2)$. Therefore every G_f-reduced element $g \in \widehat{\mathcal{S}}_m$ is reduced.

Recall that $c\alpha = \alpha c^\alpha$ for all $c \in C$ and $\alpha \in \widehat{G}$. Further

$$x^{\Delta\alpha}c = x^{\Delta\alpha c} = x^{\Delta c^{\alpha^{-1}}\alpha}$$

for all $x \in X$, $\Delta \in \widehat{U}$, $\alpha \in \widehat{G}$, $c \in C$. Therefore, for any τ as given in (8.23), we have

$$r_C(S_\tau) \supseteq \sum_{i=1}^{n} r_C(\Delta_i)^{\alpha_i} \tag{8.26}$$

We now prove the main result of this section.

Theorem 8.3.1 *Let $f \in \widehat{\mathcal{S}}_m$ be a $\widehat{T}'$-identity on $I \triangleleft R$. Then there exists a reduced $\widehat{T}'$-identity $g \in \widehat{\mathcal{S}}_m$ on I such that $f - g \in \widehat{I}_0$.*

Proof. We choose a subset $\mathcal{M} = \{\nu_j \mid 1 \leq j \leq r\}$ and a natural number s such that f is expressible in the form $f = f(x_q^{\Theta_l c_m \alpha_i})$, $x_q \in X$, where $c_m \in C$, $\alpha_i \in \widehat{G}$, the Θ_l's are monomials in $\mathcal{M}$ and $\deg \Theta_l \leq s$. Since

$$x_q^{\Theta_l c_m \alpha_i} = x_q \otimes \Theta_l c_m \alpha_i = x_q \otimes \Theta_l \alpha_i c_m^{\alpha_i} = (x_q \otimes \Theta_l \alpha_i) c_m^{\alpha_i} = x_q^{\Theta_l \alpha_i} c_m^{\alpha_i},$$

the $\widehat{T}'$-identity f can be written in the form $f = f'(x_q^{\Theta_l \alpha_i})$ for some f'. Applying Proposition 8.1.8 we obtain that there exist a strongly independent subset $\mathcal{M}_0 \subseteq D(R)$ and a finite subset $\mathcal{M}_i \subseteq D_i$ such that any monomial Θ_l is a right C-linear combination of the monomials of the form $\Delta\Omega$ where Δ is a correct monomial in $\mathcal{M}_0$ and Ω is a monomial in $\mathcal{M}_i$. By Remark 8.2.7 we see that $\alpha_i^{-1}\mathcal{M}_i\alpha_i \subseteq D_i$ for all i. Therefore f is equivalent modulo $\widehat{I}_0$ to a $\widehat{T}'$-identity f' of the form $f' = f'(x_q^{\Delta_j \alpha_i})$ where the Δ_j's are correct monomials in $\mathcal{M}_0$. Next applying Proposition 8.2.9(**ii**) (with $H = G_i$) to the set of all the α_i's and using the equalities of the form $x^{t_1+t_2} = x^{t_1} + x^{t_2}$ where $t_1, t_2 \in \widehat{T}$, we obtain that f' can be written in the form $f' = f'(x_q^{\Delta_j \alpha_s h_{is} u_{is}})$ where $s \leq i$ and $h_{is} \in G_i$. Hence f' is equivalent modulo $\widehat{I}_0$ to a $\widehat{T}'$-identity g of the form $g = g(x_q^{\Delta_j \alpha_s u_{is}})$. Since $\Delta_j = \Delta_j E(\Delta_j)$ and $E(\Delta_j)\alpha_s = \alpha_s E(\Delta_j)^{\alpha_s}$, replacing u_{is} by $u_{is}E(\Delta_j)^{\alpha_s}$ we may assume that $u_{is} \leq E(\Delta_j)^{\alpha_s}$ for all $x_q^{\Delta_j \alpha_s u_{is}}$ involved in g. Now we infer from Proposition 8.2.9(**ii**) and (**iv**) that g is a reduced $\widehat{T}'$-identity on I and the proof is thereby complete.

The following theorem is proved analogously to that of Theorem 8.3.1.

Theorem 8.3.2 *Let $f \in \widehat{S}_m$ be a $\widehat{T}'$-identity on $I \lhd R$. Then there exists a G_f-reduced $\widehat{T}'$-identity $g \in \widehat{S}_m$ on I such that $f - g \in \widehat{I}_0$.*

Finally, we touch very briefly on the situation where we are only interested in the group $G^* = Aut(S)$ rather than in the group $\widehat{G}$. The development and arguments being very similar to those used in the preceding exposition, we shall leave all details to the reader. One forms the skew group ring $\widehat{T}^* = \widehat{U} \propto G^*$, shows that there exists a C-ring homomorphism $\gamma^* : \widehat{T}^* \to End(Q)$ in a natural way, and defines *the $*$-maximal setting of* R to be

$$\widehat{\mathcal{S}}^*_m = Q \coprod_C C\{V \otimes_C \widehat{T}^*\}$$

One then defines the notions of $\widehat{T}^*$-substitution and $\widehat{T}^*$-identity (see section 7.8). Set $G^*_f(R) = G_f(R) \cap G^*(S)$. The concept of a G^*_f-reduced element of $\widehat{\mathcal{S}}^*_m$ is introduced analogously to that of a G_f-reduced element of $\widehat{\mathcal{S}}_m$. Next we define the set $\widehat{I}^*_0$ of trivial $\widehat{T}^*$-identities of R to be the ideal of $\widehat{\mathcal{S}}^*_m$ generated by all elements of the forms given by (C'_1) and (C'_2). We close this section with the following theorem which is proved similarly to that of Theorem 8.3.1

Theorem 8.3.3 *Let $f \in \widehat{\mathcal{S}}^*_m$ be a $\widehat{T}^*$-identity on $I \lhd R$. Then there exists a G^*_f-reduced $\widehat{T}^*$-identity $g \in \widehat{\mathcal{S}}^*_m$ on I such that $f - g \in \widehat{I}^*_0$.*

8.4 Semiprime Rings with $\widehat{T}'$-identities

We are now in a position to prove the analogues of the main results of Chapter 7 for semiprime rings. We begin with

Theorem 8.4.1 *Let I be a nonzero ideal of R and let $f \in \widehat{\mathcal{S}}_m$ be a $\widehat{T}'$-identity on I. Then f is a $\widehat{T}'$-identity on $E(I)Q_s$.*

Proof. Let $f = f_\rho$ where ρ is some support of f. We write $f = f(x_i^{\Delta_j \alpha_k})$ where $x_i \in X$, $i = 1, 2, \ldots, n$, $\Delta_j \in \widehat{U}$, $\alpha_k \in \widehat{G}$, and $\{\alpha_1, \ldots, \alpha_m\} \subseteq \widehat{G}$ are all the elements of $\widehat{G}$ appearing in f_ρ.

(The notation is suggestive of the fact that $(x_i, \Delta_j, \alpha_k)$ appears in some τ where $S_\tau \in \rho$). Given $1 \le i \le n$ we let A_i to be the set of all α_k's such that $x_i^{\Delta_j \alpha_k}$ is involved in f_ρ for some $j = j(i,k)$. We define

$$N_I(f_\rho) = \sum_{i=1}^{n} |\{(\alpha', \alpha'') \in A_i \times A_i \mid e^{\alpha'} \neq e^{\alpha''} \text{ for some } e \le E(I)\}|$$

Of course $N_I(f) = N_I(f_\rho)$ depends on the support ρ. Supposing that our theorem is not true, we let F to be the set of all pairs $(J,\ g,\ \sigma)$ such that:

(1) J is an nonzero ideal of R;

(2) $g \in \widehat{S}_m$ is a $\widehat{T}'$-identity on J with support σ;

(3) our theorem is not valid for the triple $(J,\ g,\ \sigma)$.

We set

$$\begin{aligned} F_1 &= \{(J,\ g,\ \sigma) \in F \mid \sigma\text{-}ht(g) + \sigma\text{-deg}(g) \quad \text{is minimal}\}, \\ F_2 &= \{(J,\ g,\ \sigma) \in F_1 \mid N_J(g) \quad \text{is minimal}\}, \quad \text{and} \\ F_3 &= \{(J,\ g,\ \sigma) \in F_2 \mid M_\sigma(g) \quad \text{is minimal}\}. \end{aligned}$$

Since our theorem is not valid for $(I,\ f,\ \rho)$, $F_3 \neq \emptyset$. Let $(J,\ g,\ \sigma) \in F_3$. Write $g = g(x_1, x_2, \ldots, x_n)$ where $x_1, x_2, \ldots, x_n \in X$ are all the variables involved in g. We make the following general remark. In what follows we shall transform g into some other $\widehat{T}'$-identities ($g', g - g', h, g_1$ and so on). In all cases it will be clear how the support σ of g induces a support of corresponding identity. With this remark in mind we shall use the simplified notations for degree, height and so on. We now claim that g vanishes under the substitution $x_i \mapsto 0$, $x_j \mapsto x_j$, $j \neq i$, where $1 \le i \le n$ is fixed. Indeed, if g' is the result of this substitution, then g' and $g - g'$ are $\widehat{T}'$-identities on J and so they are $\widehat{T}'$-identities on $E(J)Q_s$ because $M(g'), M(g - g') < M(g)$. But then we have a contradiction to the choice of $(J,\ g,\ \sigma)$. Thus our claim is established. It follows that every τ-monomial of g involves all the variables $x_1, x_2, \ldots, x_n$.

Next we claim that $n = 1$. Indeed, let $0 \leq i < n$ be such number that $g(q_1, \dots, q_i, r_{i+1}, \dots, r_n) = 0$ for all $q_1, \dots, q_i \in E(J)Q_s$ and $r_{i+1}, \dots, r_n \in J$ but $g(p_1, \dots, p_{i+1}, s_{i+2}, \dots, s_n) \neq 0$ for some $p_1, \dots, p_{i+1} \in E(J)Q_s$ and $s_{i+2}, \dots, s_n \in J$. Setting $h(x) = g(p_1, \dots, p_i, x, s_{i+2}, \dots, s_n)$, we note that by the above result $\deg(h) < \deg(g)$. Further $(J,\ h,\ \theta) \in F$ (where θ is a support of h induced by σ) and we have:

$$\begin{aligned} ht(h) + \deg(h) &< ht(g) + \deg(g), \\ N_J(h) &\leq N_J(g) \quad \text{and} \\ M(h) &\leq M(g), \end{aligned}$$

a contradiction to the choice of $(J,\ g\,\sigma)$. Therefore $n = 1$ and we can write $g = g(x)$.

We claim now that $N_J(g) > 0$. Indeed, let $N_J(g) = 0$. We write $g = g(x^{\Delta_j \alpha_k})$ where $\{\Delta_1, \dots, \Delta_l\} \subseteq \widehat{U}$ and $A = \{\alpha_1, \dots, \alpha_m\} \subseteq \widehat{G}$ are all the elements of $\widehat{U}$ and $\widehat{G}$ appearing in g. Then fixing some $\beta \in A$, we conclude that

$$v^\beta = v^\alpha$$

for all $v \leq e = E(J)$, $\alpha \in A$. We show that g is a $\widehat{T}'$-identity on $O(J)$. Let $r \in O(J)$. It is enough to show that g vanishes under the substitution $x \mapsto r$. To this end we recall from Proposition 3.1.14 that $r = \sum^{\perp}_{v \in V} r_v v$ where V is a dense orthogonal subset of B and $r_v \in J$ for all $v \in V$. Applying Remark 3.1.16 we obtain that

$$r^{\Delta_j \alpha_k} = \sum_{v \in V}{}^{\perp} r_v^{\Delta_j \alpha_k} v^{\alpha_k} = \sum_{v \in V}{}^{\perp} r_v^{\Delta_j \alpha_k} v^{\beta}$$

where $\alpha_k \in A$. (Since $\alpha_k = \alpha\beta$, $\alpha \in G$, $\beta = \sum^{\perp}_{u \in U} \beta_u u \in G_f$ one may apply Remark 3.1.16 to each β_u acting on Su). Setting $W = V^\beta$ and $r_w = r_v$ for $w = v^\beta$, we infer from Remark 3.1.8 and Remark 3.1.9 that

$$g(r^{\Delta_j \alpha_k}) = \sum_{w \in W}{}^{\perp} g(r_w^{\Delta_j \alpha_k}) w = 0$$

and hence g is a $\widehat{T}'$-identity on $O(J)$. Setting

$$\Delta'_j = \beta^{-1}\Delta_j\beta, \quad \text{and} \quad \gamma_k = \beta^{-1}\alpha_k,$$

we note that $(v^\beta)^{\gamma_k} = v^{\alpha_k} = v^\beta$ for all $v \leq E(J)$. Since $E(J^\beta) = E(J)^\beta$, we conclude that $u^{\gamma_k} = u$ for all $u \leq E(J^\beta)$. Let

$$h(x^{\Delta'_j\gamma_k}) = g(x^{\beta^{-1}\Delta_j\alpha_k}).$$

Then h is a $\widehat{T}'$-identity on $O(J)^\beta = O(J^\beta)$. Clearly g is a $\widehat{T}'$-identity on $E(J)Q_s$ if and only if h is a $\widehat{T}'$-identity on $E(J^\beta)Q_s$. Therefore without loss of generality we can assume that $\beta = 1$ and $v^\alpha = v$ for all $v \leq E(J)$ and $\alpha \in A$. It follows that

$$g((E(J)x)^{\Delta_j\alpha_k}) = E(J)g(x^{\Delta_j\alpha_k}).$$

Since $E(J)q = q$ for all $q \in E(J)Q_s$, we conclude that g is a $\widehat{T}'$-identity on $E(J)Q_s$ if and only if $E(J)g$ is a $\widehat{T}'$-identity on Q_s. Replacing g by $E(J)g$ we can assume that $E(J)g = g$.

Let $M \in Spec(B)$ with $E(J) \notin M$. Then by Corollary 8.2.12, $M^\alpha = M$ for all $\alpha \in A$. According to Lemma 8.2.10 each $\alpha_k \in A$ induces an (anti)automorphism $\overline{\alpha_k}$ of $\overline{S} = S/MS$. Denote by $\overline{\Delta_j}$ the canonical image of Δ_j in $U(\overline{S})$ and by g' the canonical image of g in $\mathcal{S}_m(\overline{S})$. Clearly $g' = g'(x^{\overline{\Delta_j}\overline{\alpha_k}})$ is a T'-identity on $\overline{S}$. It follows from Theorem 7.8.6 that g' is a T'-identity on $Q_s(\overline{S})$. Since $\overline{Q_s} \subseteq Q_s(\overline{S})$, we conclude that g' is a T'-identity on $\overline{Q_s}$. Therefore $\phi_M(g(q^{\Delta_j\alpha_k})) = 0$ for all $q \in Q_s$, $M \in Spec(B)$ with $E(J) \notin M$. Suppose now that $E(J) \in M$. Then $g(q^{\Delta_j\alpha_k}) = E(J)g(q^{\Delta_j\alpha_k}) \in MQ$ and so $\phi_M(g(q^{\Delta_j\alpha_k})) = 0$ for all $q \in Q_s$, $M \in Spec(B)$. It follows that g is a $\widehat{T}'$-identity on Q_s, a contradiction. Therefore $N_J(g) > 0$.

Next we recall that g is called additive on $E(J)Q_s$ if for all $r, s \in E(J)Q_s$ we have

$$g((r+s)^{\Delta_j\alpha_k}) = g(r^{\Delta_j\alpha_k}) + g(s^{\Delta_j\alpha_k}).$$

Supposing that g is additive on $E(J)Q_s$, we show that g is a $\widehat{T}'$-identity on $E(J)Q_s$. Since $N_J(g) > 0$, after a suitable renumbering of $\alpha_1, \ldots, \alpha_m$ we may assume that $v^{\alpha_1} \neq v^{\alpha_2}$ for some $v \leq e = E(J)$ and $\alpha_1, \alpha_2 \in A$. Applying Lemma 8.2.11 to $\alpha_1\alpha_2^{-1}$, we find pairwise orthogonal idempotents $e_0, e_1, e_2, e_3 \in B$ such that $e_0 + e_1 + e_2 + e_3 = 1$, $v^{\alpha_1\alpha_2^{-1}} = v$ for all $v \leq e_0$ and $e_i^{\alpha_1\alpha_2^{-1}} e_i = 0$ for all $i = 1, 2, 3$. Therefore

$$\begin{aligned} v^{\alpha_1} &= v^{\alpha_2} \quad \text{for all} \quad v \leq e_0; & (8.27)\\ e_i^{\alpha_1} e_i^{\alpha_2} &= 0 \quad \text{for all} \quad i = 1, 2, 3. & (8.28) \end{aligned}$$

Now we set

$$\begin{aligned} g_1 &= \text{the sum of all } \tau\text{-monomials of } g \text{ which involve} \\ &\quad\; x^{\Delta_j\alpha_1} \text{ but do not involve } x^{\Delta_k\alpha_2},\ \ \Delta_j, \Delta_k \in \widehat{U}; \\ g_2 &= \text{the sum of all } \tau\text{-monomials of } g \text{ which involve} \\ &\quad\; x^{\Delta_j\alpha_2} \text{ but do not involve } x^{\Delta_k\alpha_1},\ \ \Delta_j, \Delta_k \in \widehat{U}; \\ g_3 &= \text{the sum of all } \tau\text{-monomials of } g \text{ which involve} \\ &\quad\; \text{both } x^{\Delta_j\alpha_1} \text{ and } x^{\Delta_k\alpha_2},\ \ \Delta_j, \Delta_k \in \widehat{U}; \\ g_4 &= \text{the sum of all } \tau\text{-monomials of } g \text{ which do not} \\ &\quad\; \text{involve either } x^{\Delta_j\alpha_1} \text{ or } x^{\Delta_k\alpha_2},\ \ \Delta_j, \Delta_k \in \widehat{U}. \end{aligned}$$

Clearly $g = g_1 + g_2 + g_3 + g_4$ and $M(g) = M(g_1) + M(g_2) + M(g_3) + M(g_4)$. Now we choose a dense ideal K of R such that $e_iK \subseteq R$ for all $i = 0, 1, 2, 3$ and set $K_i = e_iKJ$. Clearly K_i is an ideal of R and $K_0 \oplus K_1 \oplus K_2 \oplus K_3 = KJ$. Therefore $E(KJ) = E(K_0) + E(K_1) + E(K_2) + E(K_3)$. Since K is a dense ideal of R, one can easily show that $r_C(KJ) = r_C(J)$ and so $E(KJ) = E(J)$. In view of additivity of g on $E(J)Q_s$, it is enough to show that g is a $\widehat{T}'$-identity on $E(K_i)Q_s$ for all $i = 0, 1, 2, 3$. To this end we note that $E(K_i) \leq e_i$ for all $i = 0, 1, 2, 3$ by Theorem 2.3.9(**ii**) because $K_i = e_iKJ$. Recalling that $v^{\alpha_1} = v^{\alpha_2}$ for all $v \leq e_0$, we obtain that $N_{K_0}(g) \leq N_J(g) - 1$.

By the choice of (J, g, σ) we have that g is a $\widehat{T}'$-identity on $E(K_0)Q_s$. Further suppose that $g_3 \neq 0$. Since $e_i^{\alpha_1}e_i^{\alpha_2} = 0$ for all $i = 1, 2, 3$, we conclude that g_3 is a $\widehat{T}'$-identity on e_iQ_s (and so $g - g_3$ is a $\widehat{T}'$-identity on K_i). On the other hand, since $M(g - g_3) < M(g)$, we infer from the choice of (J, g, σ) that $g - g_3$ is a $\widehat{T}'$-identity on $E(K_i)Q_s$. Then $g = g - g_3 + g_3$ is a $\widehat{T}'$-identity on $E(K_i)Q_s$, $i = 1, 2, 3$. Hence g is a $\widehat{T}'$-identity on $E(J)Q_s$ which contradicts the choice of (J, g, σ). Therefore $g_3 = 0$ and $g = g_1 + g_2 + g_4$. As $\alpha_1, \alpha_2 \in A$, we see that $g_1 \neq 0 \neq g_2$. Recalling that $e_ix = x$ for all $x \in K_i$ we infer that

$$g_1(x) = g_1(e_ix) = e_i^{\alpha_1}g_1(e_ix) = e_i^{\alpha_1}g_1(x)$$

for all $x \in K_i$, $i = 1, 2, 3$. Analogously one can show that $g_2(x) = e_i^{\alpha_2}g_2(x)$ for all $x \in K_i$, $i = 1, 2, 3$. Since $e_i^{\alpha_1}e_i^{\alpha_2} = 0$ for $i = 1, 2, 3$, we conclude that $e_i^{\alpha_1}g_2$ (and so $e_i^{\alpha_1}g_1 + e_i^{\alpha_1}g_4$) is a is $\widehat{T}'$-identity on K_i, $i = 1, 2, 3$. Since $M(e_i^{\alpha_1}g_2) < M(g)$ and $M(e_i^{\alpha_1}g_1 + e_i^{\alpha_1}g_3) < M(g)$, we conclude that they are $\widehat{T}'$-identities on $E(K_i)Q_s$. Therefore $e_i^{\alpha_1}g$ is a $\widehat{T}'$-identity on $E(K_i)Q_s$. On the other hand $(1 - e_i^{\alpha_1})g_1$ (and hence $(1 - e_i^{\alpha_1})g_2 + (1 - e_i^{\alpha_1})g_3)$ is a $\widehat{T}'$-identity on K_i. So they are $\widehat{T}'$-identities on $E(K_i)Q_s$. Therefore $(1 - e_i^{\alpha_1})g$ is a $\widehat{T}'$-identity on $E(K_i)Q_s$. It is clear now that g is a $\widehat{T}$-identity on $E(K_i)Q_s$. Therefore g is a $\widehat{T}'$-identity on $E(K)Q_s = E(J)Q_s$ which contradicts the choice of (J, g, σ). Thus g is not additive on $E(J)Q_s$. In particular g is not multilinear and $ht(g) > 0$.

Let $y \in X$ be any variable distinct from x. We consider $q(y) = g(x + y) - g(x) - g(y)$. Obviously q is a $\widehat{T}'$-identity on J and $ht(q) < ht(g)$. Therefore q is a $\widehat{T}'$-identity on $E(J)Q_s$ and so g is additive on $E(J)Q_s$, a contradiction. The proof is complete.

Analogously one can prove the following

Theorem 8.4.2 *Let I be a nonzero ideal of R and let $f \in \widehat{S}_m^*$ be a $\widehat{T}^*$-identity on I. Then f is a $\widehat{T}^*$-identity on $E(I)Q_s$.*

The following technical lemma will be needed in the proofs of the remaining theorems.

Lemma 8.4.3 *Let $A = \{\alpha_1, \alpha_2, \ldots, \alpha_m\} \subseteq \widehat{G}$, $M \in Spec(B)$, and $\{M_1, M_2, \ldots, M_r\} = \{M^{\alpha^{-1}} \mid \alpha \in A\}$ where $M_i \neq M_j$ for $1 \leq i \neq j \leq r$. Choose $\beta_1, \beta_2, \ldots, \beta_r \in A$ such that each $M_i = M^{\beta_i^{-1}}$, let β_{i_k} denote the unique β_j for which $M^{\alpha_k^{-1}} = M^{\beta_{i_k}^{-1}}$, and set $\alpha_k = \beta_{i_k}\gamma_k$. Furthermore let $\Delta \in \widehat{U}$, $h \in G_f$, $v \in B$, and let $z_1, z_2, \ldots, z_r$ be distinct variables in X. Then there exists $e \in B$ such that*

$$\begin{aligned} e &\notin M, \\ e^{\beta_i^{-1}} e^{\beta_j^{-1}} &= 0 \quad \textit{for all } 1 \leq i \neq j \leq r, \\ e^{\gamma_k} &= e \quad \textit{for all } k = 1, 2, \ldots, m \end{aligned}$$

and, if $z = \sum_{i=1}^{r} z_i e^{\beta_i^{-1}}$ then

$$ez^{\Delta\alpha_k hv} = ez_{i_k}^{\Delta\alpha_k hv}.$$

Proof. We first note that $M^{\gamma_k} = M$. According to Corollary 8.2.12 there exists an idempotent $w_k \in B$ such that $w_k \notin M$ and $v^{\gamma_k} = v$ for all $v \leq w_k$. We set $w = w_1 w_2 \ldots w_k$, and note that $w \notin M$ and $v^{\gamma_k} = v$ for all $v \leq w$, $k = 1, 2, \ldots, m$. Applying the Chinese Reminder Theorem to the Boolean ring B and distinct maximal ideals $M_1, M_2, \ldots, M_r$, we find idempotents $e_1, e_2, \ldots, e_r \in B$ such that $e_i \notin M_i$ and $e_i \in M_s$ for all i, s with $1 \leq i \neq s \leq r$. Replacing each e_i by $e_i \prod_{s \neq i}(1 - e_s)$, we can also assume that $e_i e_s = 0$ for all $i \neq s$. Since $M_i^{\beta_i} = M$, we see that $e_i^{\beta_i} \notin M$ and $e_i^{\beta_s} \in M$ for all $i \neq s$. Set $e = e_1^{\beta_1} e_2^{\beta_2} \ldots e_r^{\beta_r} w$. Then

$$\begin{aligned} e &\notin M, && (8.29) \\ e^{\beta_i^{-1}} e^{\beta_s^{-1}} &= 0 \quad \text{for all } i \neq s, && (8.30) \\ e^{\gamma_k} &= e \quad \text{for all } k = 1, 2, \ldots, m && (8.31) \end{aligned}$$

because $e^{\beta_i^{-1}}e^{\beta_s^{-1}} \leq e_ie_s = 0$ and $e \leq w_k$ for all $k = 1, 2, \dots, m$. Finally, we see that

$$\begin{aligned}
ez^{\Delta\alpha_k hv} &= z^{\Delta\alpha_k hve} = z^{\Delta\alpha_k ehv} \\
&= z^{\Delta\beta_{i_k}\gamma_k ehv} = z^{\Delta e^{\beta_{i_k}^{-1}}\beta_{i_k}\gamma_k hv} \\
&= \left(\sum_{i=1}^{r} z_i e^{\beta_i^{-1}}\right)^{e^{\beta_{i_k}^{-1}}\Delta\beta_{i_k}\gamma_k hv} = z_{i_k}^{\Delta e^{\beta_{i_k}^{-1}}\beta_{i_k}\gamma_k hv} \\
&= z_{i_k}^{\Delta\alpha_k hve} = ez_{i_k}^{\Delta\alpha_k hv}
\end{aligned}$$

making use of (8.30) and (8.31). The proof is now complete.

Theorem 8.4.4 *Let $0 \neq I \lhd R$ and let $f(x_i^{\Delta_j\alpha_k h_l v_t})$ be a G_f-reduced $\widehat{T}'$-identity on I. Set $u_{kt} = v_tE(I)^{\alpha_k}$ and choose distinct elements $y_{ijk} \in X$. Then $f(y_{ijk}^{h_l}u_{kt})$ is a G_f-reduced $\widehat{T}'$-identity on Q_s.*

Proof. In what follows we shall consider G_f-reduced $\widehat{T}'$-identities. It will be understood that each identity is reduced with respect to some (attached) support and so we will simply write deg, *ht* and so on in place of, respectively, ρ-deg, ρ-*ht* and so on. We shall transform some of these identities into other ones. It will be also understood that the supports of resulting identities are induced by the supports of initial ones in a natural way.

It follows from Theorem 8.4.1 that f is a $\widehat{T}'$-identity on $E(I)Q_s$. Hence without loss of generality we can assume that $R = Q_s$ and $I = eQ_s$ for some $e \in B$. Then $E(I) = e$. Recall that $e^{h_l} = e$ for all $e \in B$ (see Corollary 8.2.3). Clearly $f((x_ie)^{\Delta_j\alpha_k h_l v_t})$ is a $\widehat{T}'$-identity on Q_s. Now replacing f by $f(x_i^{\Delta_j\alpha_k h_l v_t}e^{\alpha_k})$ we can assume that f is a G_f-reduced $\widehat{T}'$-identity (with respect to some representation ρ) on Q_s. We show that $f(y_{ijk}^{h_l}v_t)$ is a $\widehat{T}'$-identity on Q_s. Suppose that the theorem is not true for f. Let F be the set of all the G_f-reduced $\widehat{T}'$-identities on Q_s for which the theorem does not hold. We set

$$\begin{aligned} F_1 &= \{g \in F \mid \deg(g) \quad \text{is minimal}\}, \quad \text{and} \\ F_2 &= \{g \in F_1 \mid M(g) \quad \text{is minimal}\}, \end{aligned}$$

and note that $F_2 \neq \emptyset$. Without loss of generality we can assume that $f \in F_2$.

Write $f = f(x_1, x_2, \ldots, x_n)$ where $x_1, x_2, \ldots, x_n \in X$ are all the variables involved in f. We claim that g vanishes under the substitution $x_p \mapsto 0$, $x_q \mapsto x_q$, $q \neq p$, where $1 \leq p \leq n$ is fixed. Indeed, if g is the result of this substitution, then g and $f - g$ are G_f-reduced $\widehat{T}'$-identities on Q_s. Clearly $M(g), M(f - g) < M(f)$. Therefore our theorem is valid for g and $f - g$. Hence it is valid for $f = f - g + g$, a contradiction. Thus our claim is established. It follows that every τ-monomial of g involves all the variables $x_1, x_2, \ldots, x_n$.

Next we claim that $n = 1$. Suppose that $n > 1$. Choose the maximal integer r such that $0 \leq r \leq n$ and $f(y_{ijk}^{h_l} v_t)$ vanishes under all the substitutions of the form $y_{ijk} \mapsto q_{ijk}$, $i \leq r$, and $y_{ijk} \mapsto d_i^{\Delta_j \alpha_k h_l}$, $i > r$, where $d_i, q_{ijk} \in Q_s$. Since $f(y_{ijk}^{h_l} v_t)$ is not a $\widehat{T}'$-identity on Q_s, $r < n$. Hence $f(y_{ijk}^{h_l} v_t)$ does not vanish for some substitution $y_{ijk} \mapsto q_{ijk}$, $i \leq r + 1$, and $y_{ijk} \mapsto d_i^{\Delta_j \alpha_k h_l}$, $i > r+1$, where $d_i, q_{ijk} \in Q_s$. Denote by $h(x^{\Delta_j \alpha_k h_l v_t})$ the element obtained from $f(y_{ijk}^{h_l} v_t)$ via the substitution $y_{ijk} \mapsto q_{ijk}$, $i \leq r$, $y_{(r+1)jk} \mapsto x^{\Delta_j \alpha_k h_l}$, and $y_{ijk} \mapsto d_i^{\Delta_j \alpha_k h_l}$, $i > r + 1$. Clearly h is a G_f-reduced $\widehat{T}'$-identity on Q_s and $h(q_{(r+1)jk}^{h_l} v_t) \neq 0$. On the other hand, $h(x^{\Delta_j \alpha_k h_l v_t})$ is a G_f-reduced $\widehat{T}'$-identity on Q_s and $\deg(h) < \deg(f)$ because every τ-monomial of f involves each variable x_i. By the choice of f, $h(y_{jk}^{h_l} v_t)$ is a $\widehat{T}'$-identity on Q_s, a contradiction to $h(q_{(r+1)jk}^{h_l} v_t) \neq 0$. Thus our claim is proved. We set $x = x_1$ and write $f = f(x^{\Delta_j \alpha_k h_l v_t})$. Let $A = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ and $\{\Delta_1, \Delta_2, \ldots, \Delta_{m'}\}$ be all the elements of $\widehat{G}(R)$ and $\widehat{U}(R)$ respectively involved in f.

Choose any $q_{jk} \in Q_s$. It is enough to show that $f(q_{jk}^{h_l}v_t) = 0$. It follows from the definition of a Frobenius element and the fact that only a finite number of h_l's are involved in f that there exists a dense orthogonal subset $V \subseteq B$ such that $h_l v$ is a Frobenius (anti)automorphism of Sv for all $v \in V$ and l. We claim that it is enough to show that $\phi_M(f(q_{jk}^{h_l}v_t)) = 0$ for all $M \in Spec(B)$ with $V \not\subseteq M$. Indeed, suppose that $\phi_M(f(q_{jk}^{h_l}v_t)) = 0$ for all $M \in Spec(B)$ with $V \not\subseteq M$. Setting $e = E(f(q_{jk}^{h_l}v_t))$, we infer from Corollary 3.2.4 that $\phi_M(f(q_{jk}^{h_l}v_t)) = 0$ if and only if $e \in M$. It follows that the condition $V \not\subseteq M$ implies that $e \in M$. Suppose that $e \neq 0$. Since V is dense, there exists $v \in V$ such that $ve \neq 0$. Choose $M \in Spec(B)$ such that $ve \notin M$. Then $v, e \notin M$. It follows that $V \not\subseteq M$, but $e \notin M$, a contradiction. Hence $e = 0$ and our claim is established.

Fix any $M \in Spec(B)$ such that $V \not\subseteq M$ and $\phi_M(f(q_{jk}^{h_l}v_t)) \neq 0$. Suppose first that $M^{\alpha_i^{-1}} = M^{\alpha_j^{-1}}$ for all $\alpha_i, \alpha_j \in A$. Then fixing some $\beta \in A$, we see that $M^{\beta^{-1}} = M^{\alpha^{-1}}$ for all $\alpha \in A$. Setting

$$\Delta_j' = \beta^{-1}\Delta_j\beta, \quad \gamma_k = \beta^{-1}\alpha_k,$$

we note that $\alpha_k = \beta\gamma_k$ and

$$\Delta_j'\gamma_k h_l v_t = \beta^{-1}\Delta_j\alpha_k h_l v_t.$$

Therefore

$$h(x^{\Delta_j'\gamma_k h_l v_t}) = f(x^{\beta^{-1}\Delta_j\alpha_k h_l v_t})$$

is a $\widehat{T}'$-identity on Q_s. Clearly h is a G_f-reduced $\widehat{T}'$-identity on Q_s. Next we note that $M^{\gamma_k} = M$ for all γ_k. Therefore γ_k induces an (anti)automorphism $\overline{\gamma_k}$ of $\overline{S}$ (see Lemma 8.2.10). We now let h' be the element of $\widehat{S}_m$ obtained from h by deleting all τ-monomials in which some v_t with $v_t \in M$ appears. We see that h' remains a G_f-reduced element of $\widehat{S}_m$ (here we note that h' is not a $\widehat{T}'$-identity in general). Letting $A' = \{\gamma_k \mid \gamma_k \text{ appears in } h'\}$, we claim that $\overline{\gamma_k} \not\equiv \overline{\gamma_l}$ $(mod\ G_f(\overline{S}))$ for all $\gamma_k \neq \gamma_l \in A'$. Indeed, setting $\gamma = \gamma_k^{-1}\gamma_l$, suppose $\overline{\gamma} \in G_i(\overline{S})$. By Lemma 8.2.16 there is an idempotent $e \in M$ such that $\gamma e = \sigma e$ for some $\sigma \in G_f$. But $v_{t'}$ and $v_{t''}$ (which appear respectively with γ_k and γ_l) do not belong to M by the definition of h' and A', and so $w = ev_{t'}v_{t''} \notin M$. In particular $w \neq 0$. Thus $\gamma_k^{-1}\gamma_l w = \sigma w$, or, $\gamma_l w = \gamma_k \sigma w$, a contradiction to γ_k, γ_l being completely distinct on $v_{t'}v_{t''}$ modulo G_f. Next, according to Corollary 8.2.3, $e^{h_l} = e$ for all $e \in B$ and h_l appearing in h. In particular $M^{h_l} = M$ and so h_l induces an (anti)automorphism $\overline{h_l}$ of $\overline{S}$. Since $V \not\subseteq M$, $\overline{h_l}$ is a Frobenius (anti)automorphism of $\overline{S}$. We claim that $\overline{h_l} \not\equiv \overline{h_s}$ $(mod\ G_i(\overline{S}))$ for all $h_l \neq h_s$ appearing in h'. Indeed, letting $g = h_l^{-1}h_s \in G_f$, suppose that $\overline{g} = inn(b) \in G_i(\overline{S})$. Hence $0 \neq b \in M_{\overline{g}}$. By Corollary 8.2.15 $ge = \rho e$ for some $\rho \in G_i$. Now, from $w = ev_{t'}v_{t''} \notin M$ we have $h_l w = h_s \rho w$, in contradiction to h_l, h_s being completely distinct on $v_{t'}v_{t''}$ modulo G_i. Next we denote by $\overline{\Delta_j}'$ the canonical image of Δ_j' in $U(D(\overline{S}))$ and by $\overline{h}'$ the canonical image of h' in $\mathcal{S}_m(\overline{S})$. It follows from the definition of h' that $\overline{h}' = \overline{h}$. Applying Lemma 8.1.7 **(i)** to $\{\overline{\Delta_j}'\}$ we see that $\overline{h}'$ is a reduced T'-identity of $\overline{S}$ (since $\overline{h}' = \overline{h}$). It follows from Theorem 7.8.5 that

$$\phi_M(f(q_{jk}^{h_l}v_t)) = \phi_M(h'((q_{jk}^{\beta})^{h_l}v_t)) = 0,$$

a contradiction.

Now let $\{M_1, M_2, \ldots, M_r\} = \{M^{\alpha^{-1}} \mid \alpha \in A\}$ where $M_i \neq M_j$ for $1 \leq i \neq j \leq r$. By the above result $r > 1$. With reference to Lemma 8.4.3 (and its notations) we set $z = \sum_{i=1}^{r} z_i e^{\beta_i^{-1}}$ (z_i's are distinct elements of X) and $g = ef(z_{i_k}^{\Delta_j \alpha_k h_l v_t})$. By Lemma 8.4.3 $e \notin M$ and g is a G_f-reduced $\widehat{T}'$-identity on Q_s. Clearly $M(g) \leq M(f)$ and $\deg(g) \leq \deg(f)$. Suppose that our theorem is valid for g, that is $ef(y_{i_k jk}^{h_l} v_t)$ is a $\widehat{T}'$-identity on Q_s. Then making use of the substitution $y_{i_k jk} \mapsto q_{jk}$ we see that $ef(q_{jk}^{h_l}v_t) = 0$. Since $e \notin M$, $\phi_M(e) = 1$ and so $\phi_M(f(q_{jk}^{h_l}v_t)) = \phi_M(ef(q_{jk}^{h_l}v_t)) = 0$, a contradiction. Hence our theorem is not valid for g and so $g \in F$. As $M(g) \leq M(f)$ and $\deg(g) \leq \deg(f)$, we conclude that $g \in F_2$. Then by the above result $z_i = z_j$ for all $i, j = 1, 2, \dots, r$, a contradiction to $r > 1$. The proof is now complete.

There is an analogue of Theorem 8.4.4 for reduced $\widehat{T}'$-identities.

Theorem 8.4.5 *Let I be a nonzero ideal of R and let $f(x_i^{\Delta_j \alpha_k v_t})$ be a reduced $\widehat{T}'$-identity on I. Set $u_{kt} = v_t E(I)^{\alpha_k}$ and choose distinct elements $y_{ij} \in X$. Then $f(y_{ij}^{\alpha_k} u_{kt})$ is a reduced $\widehat{T}'$-identity on Q_s. Furthermore if f is a strict $\widehat{T}'$-identity on R, then $f(y_{ij}^{\alpha_k} v_t)$ is a strict $\widehat{T}'$-identity on Q_s.*

Proof. The proof essentially follows the same series of steps as in the proof of Theorem 8.4.4 but is simpler because only G_i (rather than both G_i and G_f) is involved. Because of this we omit the details and merely indicate any adjustments and simplifications are to be made. We first make an observation in case R is prime. We write $\alpha_k = \beta_k h_k$ where $h_k \in G_f$ and for all k, r either $\beta_k = \beta_r$ or $\beta_k \notin \beta_r G_f$. Choose distinct $z_{ij\beta_k} \in X$. Then applying Theorem 7.8.6 to the reduced T'-identity $f(x_i^{\Delta_j \beta_k h_k})$, we conclude that $f(z_{ij\beta_k}^{h_k})$ is a T'-identity on Q_s. Making use of the substitution $z_{ij\beta_k} \mapsto y_{ij}^{\beta_k}$, we see that $f(y_{ij}^{\alpha_k})$ is a T'-identity on Q_s.

To outline the proof one may assume f is a reduced $\widehat{T}'$-identity on Q_s such that $f \in F_2$ and consequently of the form $f(x^{\Delta_j \alpha_k v_t})$. Choose any $q_j \in Q_s$, fix $M \in Spec(B)$ and suppose $\phi_M(f(q_j^{\alpha_k} v_t)) \neq 0$. Suppose first (the case $r = 1$) that $M^{\alpha_k^{-1}} = M^{\beta^{-1}}$ for some fixed β and all α_k. Setting $\Delta_j' = \beta^{-1} \Delta_j \beta$ and $\gamma_k = \beta^{-1} \alpha_k$, we have $h(x^{\Delta_j' \gamma_k v_t}) = f(x^{\beta^{-1} \Delta_j \alpha_k v_t})$ is a reduced $\widehat{T}'$-identity on Q_s. Using Corollary 8.2.15, one shows that $\overline{\gamma_l} \not\equiv \overline{\gamma_s}$ modulo $G_i(\overline{S})$ for all $\gamma_l \neq \gamma_s$. Thus $\overline{h} = \overline{h}(x^{\overline{\Delta_j}' \overline{\gamma_k} \overline{v_t}})$ is a reduced T'-identity on $\overline{Q_s}$ whence by the above observation one reaches the contradiction $0 = \phi_M(h((q_j^{\beta})^{\overline{\Delta_j}' \overline{\gamma_k} \overline{v_t}})) = \phi_M(f(q_j^{\alpha_k} v_t))$. The case $r > 1$ with the assistance of Lemma 8.4.3 leads to $g = ef(z_{i_k}^{\Delta_j\alpha_k v_t})$ being a reduced $\widehat{T}'$-identity on Q_s, and a contradiction is reached in the same manner as at the end of the proof of Theorem 8.4.4.

Suppose now that f is strict. Since $E(R) = 1$, we conclude that $f(y_{ij}^{\alpha_k}v_t)$ is a $\widehat{T}'$-identity on Q_s. Since $f(x_i^{\Delta_j\alpha_k v_t})$ can be obtained from $f(y_{ij}^{\alpha_k}v_t)$ via the substitution $x_i^{\Delta_j}$ for y_{ij}, we see that $r_C(f(y_{ij}^{\alpha_k}v_t)) = r_C(f(x_i^{\Delta_j\alpha_k v_t})) = 0$. The proof is complete.

The same arguments as in the proof of Theorem 8.4.4 yield the following

Theorem 8.4.6 *Let $0 \neq I \lhd R$ and let $f(x_i^{\Delta_j\alpha_k h_l v_t})$ be a G_f^*-reduced $\widehat{T}^*$-identity on I. Set $u_{kt} = v_tE(I)^{\alpha_k}$ and choose distinct elements $y_{ijk} \in X$. Then $f(y_{ijk}^{h_l}u_{kt})$ is a $\widehat{T}^*$-identity on Q.*

Theorem 8.4.7 *Let $f(x_i^{\Delta_j\alpha_k v_t})$ be a strict reduced $\widehat{T}'$-identity on R. Then R has a strict GPI $g \in Q_C{<}X{>}$.*

Proof. Let $A = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be all the elements of $\widehat{G}(R)$ involved in f. Next let $\{x_1, x_2, \dots, x_m\}$ be all the variables involved in f. By Theorem 8.4.1 f is a $\widehat{T}'$-identity on S. In view of Theorem 8.4.5 we can assume that $f = f(x_j^{\alpha_k v_t})$. According to Corollary 6.3.10 it is enough to show that $\phi_M(S)$ is GPI for all $M \in Spec(B)$. Fix any $M \in Spec(B)$ and assume that $\overline{S} = \phi_M(S)$ is not GPI.

Let $\{M_1, M_2, \dots, M_r\} = \{M^{\alpha^{-1}} \mid \alpha \in A\}$ where $M_i \neq M_j$ for all $i, j = 1, 2, \dots, r$ and $r \geq 1$. Choose $\beta_1, \dots, \beta_k \in A$ such that $M^{\beta_i^{-1}} = M_i$ for $i = 1, 2, \dots, r$. It follows from Lemma 8.4.3 applied to each variable x_j that there exist $e \notin M$ and $z_{ji_k} \in X$ such that $ef(z_{ji_k}^{\alpha_k v_t})$ is a $\widehat{T}'$-identity on S and $z_{ji_k} = z_{li_s}$ if and only if $j = l$ and $i_k = i_s$. Note that i_k is given by the condition $M^{\alpha_k^{-1}} = M^{\beta_{i_k}^{-1}}$. Making use of the substitution $z_{ji_k} \mapsto z_{ji_k}^{\beta_{i_k}^{-1}}$, we obtain that $ef(z_{ji_k}^{\beta_{i_k}^{-1}\alpha_k v_t})$ is a $\widehat{T}'$-identity on S. Set $\gamma_{i_k k} = \beta_{i_k}^{-1}\alpha_k$. Then $ef(z_{ji_k}^{\gamma_{i_k k} v_t})$ is a $\widehat{T}'$-identity on S. Clearly $M^{\gamma_{i_k k}} = M$ for all $\gamma_{i_k k}$. It follows from Corollary 8.2.12 that there exists an idempotent $w \in B \setminus M$ such that $u^{\gamma_{i_k k}} = u$ for all $u \leq w$ and $\gamma_{i_k k}$. As $ew \notin M$, $\phi_M(ewS) = \phi_M(S)$. Therefore replacing S by ewS we may assume that $ew = 1$ and so $f(z_{ji_k}^{\gamma_{i_k k} v_t})$ is a $\widehat{T}'$-identity on S. Furthermore we may assume that $u^{\gamma_{i_k k}} = u$ for all $u \leq w$ and $\gamma_{i_k k}$. Since $f(x_j^{\alpha_k v_t})$ can be obtained from $f(z_{ji_k}^{\gamma_{i_k k} v_t})$ under the substitution $z_{ji_k} \mapsto x_j^{\beta_{i_k}}$,

$$r_C(f(z_{ji_k}^{\gamma_{i_k k} v_t})) \subseteq r_C(f(x_j^{\alpha_k v_t})) = 0$$

and so $f(z_{ji_k}^{\gamma_{i_k k} v_t})$ is a strict $\widehat{T}'$-identity on S. Next, it follows from Lemma 8.2.10(**ii**) that each $\gamma_{i_k k}$ induces an (anti)automorphism $\overline{\gamma_{i_k k}}$ of $\overline{S} = \phi_M(S)$. Therefore $f(z_{ji_k}^{\gamma_{i_k k} v_t})$ induces a nonzero T'-identity $\overline{f}(z_{ji_k}^{\overline{\gamma_{i_k k}}\,\overline{v_t}})$ of $\overline{S}$. Choose any variable z_{ji_k} appearing in $\overline{f}$. First assume that there exist elements $q_{j'i_{k'}} \in \overline{S}$, $(j', i_{k'}) \neq (j, i_k)$, such that the element $g(z_{ji_k}^{\overline{\gamma_{i_{k'} k'}}\,\overline{v_{t'}}})$ obtained from $\overline{f}(z_{li_r}^{\overline{\gamma_{i_r r}}\,\overline{v_t}})$ under the substitution $z_{j'i_{k'}} \mapsto q_{j'i_{k'}}$, $(j', i_{k'}) \neq (j, i_k)$, is nonzero. Here we note that the appearance of $z_{ji_k}^{\overline{\gamma_{i_{k'} k'}}}$ in g means that $i_{k'} = i_k$, i.e., $\gamma_{i_{k'} k'} = \beta_{i_k}^{-1}\alpha_{k'}$. Clearly g is a T'-identity on $\overline{S}$. We claim that g is a reduced T'-identity. Indeed, suppose that both $z_{ji_k}^{\overline{\gamma_{i_{k'} k'}}}$ and $z_{ji_k}^{\overline{\gamma_{i_{k''} k''}}}$ are involved in g with $\gamma_{i_{k'} k'} \neq \gamma_{i_{k''} k''}$. Then their accompanying idempotents $v_{t'}$ and $v_{t''}$ do not belong to M and so $v_{t'} v_{t''} \notin M$. By (R_3) $\alpha_{k'}$ and $\alpha_{k''}$ are completely distinct on $v_{t'} v_{t''}$ modulo G_i. Hence $\gamma_{i_{k'} k'} = \beta_{i_k}^{-1}\alpha_{k'}$ and $\gamma_{i_{k''} k''} = \beta_{i_k}^{-1}\alpha_{k''}$ are completely distinct on $v_{t'} v_{t''}$ modulo G_i. Therefore $\gamma_{i_{k''} k''}^{-1}\gamma_{i_{k'} k'} u \notin G_i u$ for all $u \leq v_{t'} v_{t''}$. It follows from Corollary 8.2.15 that $\overline{\gamma_{i_{k''} k''}}^{-1}\overline{\gamma_{i_{k'} k'}} \notin G_i(\overline{S})$ which proves our claim. We conclude now from Theorem 7.8.4 that $\overline{S}$ is GPI, a contradiction to our assumption.

By the above result $\overline{f}(z_{li_r}^{\overline{\gamma_{i_r r}}}\overline{v_t})$ vanishes under substitutions $z_{j'i_{k'}} \mapsto q_{j'i_{k'}}$, $(j', i_{k'}) \neq (j, i_k)$, where $q_{j'i_{k'}} \in \overline{S}$. We replace each appearance of $z_{ji_k}^{\overline{\gamma_{i_s s}}}$ (where $i_s = i_k$) in $\overline{f}$ by z_{ji_k} and denote by g the resulting element. Clearly g is a strict T'-identity on $\overline{S}$. Continuing in this fashion we obtain that $\overline{f}(z_{li_r}\overline{v_t})$ is a nonzero GPI on $\overline{S}$, a contradiction to our assumption. The proof is complete.

A variant of Theorem 8.4.4 for $\widehat{T}'$-identities of semiprime rings involving no (anti)automorphisms was discovered by Kharchenko in [147, Theorem 2]. Further a version of Theorem 8.4.5 for multilinear $\widehat{T}^*$-identities was proved by him in [147, Theorem 4]. To the best our knowledge all the results of this section are new. They were proved by Beidar.

Chapter 9

Applications to Lie Theory

The main goal of this chapter is to present the solution of a long-standing question of Herstein [113] on Lie isomorphisms: if R, R' are simple rings with involution with respective skew elements K, K' and $\alpha : K \to K'$ is a Lie isomorphism, then can α be extended to an isomorphism $\sigma : R \to R'$? This we accomplish in section 9.4, restricting our attention to involutions of the first kind (to be defined presently) but on the other hand widening the context to prime rings. The reason for including this topic in this book is that, although it would appear on the surface to have no special connection with GPI theory, GPI theory in fact plays a crucial role in key parts of the proof. In preparation for this, and also another application of GPI theory, we redo in section 9.1 some of Herstein's Lie theory for the important case of prime rings with involution of the first kind. In section 9.2 we determine the Lie extended centroid of K. It is not our intent to give a complete treatment of these matters but rather to show how GPI theory is used. In section 9.3, again using GPI theory in a crucial way, we prove a result on commuting traces of trilinear mappings which is crucial for the solution of the Lie isomorphism problem in section 9.4. This work was inspired by Bresar's study of commuting traces of bilinear mappings [63] which he used to settle Herstein's conjecture on Lie isomorphisms of prime rings (without involution).

9.1 The Structure of K

An associative ring R becomes a Jordan ring $R^{(+)}$ under $x \circ y = xy + yx$ and a Lie ring $R^{(-)}$ under $[x, y] = xy - yx$. In case R has an involution $*$ the set of *symmetric* elements

$$S = S(R) = \{s \in R \mid s^* = s\}$$

is a Jordan subring of $R^{(+)}$ and the set of *skew* elements

$$K = K(R) = \{k \in R \mid k^* = -k\}$$

is a Lie subring of $R^{(-)}$. In the early 1950's Herstein initiated a study of the Jordan and Lie ideals of R, S, and K in case that R was a simple associative ring (either without or with an involution). In the ensuing years his work was generalized in various directions, on the one hand to the setting of prime and semiprime rings, and, on the other hand to invariance conditions other than that given by ideals. Besides Herstein himself we mention Lanski as having been a major force in this program. Other important contributions were made by Baxter, Chacron, Erickson, Montgomery, Osborn, and others. Of particular interest to us because of the theme of this book, the GPI and PI theory for prime rings with involution has witnessed results of Amitsur [6], [7], Herstein [114], Lanski [159], [163], Martindale [207], [208], Rowen [257] and others. In fact, to pinpoint the key result in GPI theory from which all applications in this chapter are based, we recall from section 6.2 Corollary 6.2.5.

Corollary 9.1.1 *If R is a prime ring of $char(R) \neq 2$ with involution and K is GPI, then R is GPI.*

Let R be a prime ring of $char(R) \neq 2$ with involution $*$, let Ω be the centroid of R and let C be the extended centroid of R. For simplicity we shall assume that $1/2 \in \Omega$, whence we may write $R = S + K$. It is a straightforward exercise to directly lift $*$ to an involution of RC. However, this is virtually a special case of Proposition 2.5.4 which says (in its proof) that $*$ can be lifted to an antiautomorphism $*$ of the symmetric ring of quotients $Q = Q_s(R)$ such that $q^*u^* = (uq)^*$, where $0 \neq U \lhd R$ is such that $qU + Uq \subseteq R$. Thus $q^{**}u = (u^*q^*)^* = (qu)^{**} = qu$ and so $q^{**} = q$ and $*$ is an involution of Q. Since C is the center of Q, $*$ induces an involution on C and hence on the central closure RC. We shall say that $*$ is *of the first kind* if it induces the identity mapping on C. Otherwise it is *of the second kind*, which is equivalent to saying that C contains a nonzero skew element. An example of Kaplansky shows that an involution of the second kind may well act as the identity on the center: R is the set of all countably infinite matrices of the form $A + \lambda I$, A is $n \times n$ matrix over the complexes $\mathcal{C}$, n varies, $\lambda \in \mathcal{R}$ where $\mathcal{R}$ is the real number field, and $*$ is conjugate transpose (one notes that $C = \mathcal{C}$ and $Z = \mathcal{R}$).

In this section we shall (with the exception of Lemma 9.1.5 and Theorem 9.1.10) confine our attention to the study of prime rings with involution of the first kind, mainly because this is the framework in which sections 9.3 and 9.4 reside. It is generally regarded as the more difficult case, since (roughly speaking) many problems arising with an involution of the second kind may be reduced to problems in $R^{(-)}$ (where the connection with associative theory is much easier). For a complete account of Lie theory of prime rings (with or without involution), especially from the point of view of GPI theory, we refer the reader to [219].

For the remainder of this section, then, R will denote a prime ring with involution $*$ of the first kind. A Lie ideal U of K is generally defined to be an additive subgroup of K such that $[u, x] \in U$ for all $u \in U$, $x \in K$. To avoid some minor technicalities we shall also require that U be an Ω-submodule of K, where Ω is the centroid of R. We will use the notation $U \triangleleft K$ to signify that U is a Lie ideal of K. K is called a *simple Lie ring* if it has no Lie ideals other than 0 and K and $[K,K] \neq 0$ (hence $K = [K,K]$). If I is any $*$-ideal of R (i.e., an ideal invariant under $*$), then $[I \cap K, K]$ is always a Lie ideal of K, which we shall call a *standard* Lie ideal of K. We shall call a subset X of R *trivial* (notationally, $X \equiv 0$) if $[X,K] = 0$. Our major aim in this section is, given a nontrivial Lie ideal U of K, to produce a nontrivial standard Lie ideal $[I_U \cap K, K]$ lying inside K. We shall see that with the exception of two isolated "low–dimensional" cases this is possible.

For an additive subgroup W of a ring T we let $\langle W \rangle$ denote the subring of T generated by W. We will also use the following notation for higher commutators:

$$W^{(1)} = [W,W], \quad W^{(i+1)} = [W^{(i)}, W^{(i)}].$$

We begin with an easy but useful general lemma.

Lemma 9.1.2 *If W is an additive subgroup of a ring T, then $[\langle W \rangle, T] = [W,T]$.*

Proof. For $x, y \in W$ and $t \in T$ we note that

$$[xy,t] = [x,yt] + [y,tx] \in [W,T].$$

An easy induction then completes the proof.

We apply this result to the ring R.

Lemma 9.1.3 *If $U \triangleleft K$, then:*

(a) $\langle U \rangle \cap K \triangleleft K$;

(b) $[\langle U \rangle \cap K, K] \subseteq U$.

Proof. (a) follows from the observation that for $k \in K$ and $u_1, u_2, \ldots, u_n \in U$,

$$[u_1u_2 \ldots u_n, k] = \sum_i u_1u_2 \ldots [u_i, k] \ldots u_n \in \langle U \rangle.$$

Using Lemma 9.1.2 one notes that

$$[\langle U \rangle \cap K, K] \subseteq [\langle U \rangle, R] \subseteq [U, R] \subseteq [U, K] + [U, S] \subseteq U \oplus S.$$

Therefore $[\langle U \rangle \cap K, K] \subseteq U$.

It will be useful to produce a nonzero ideal inside $\langle K \rangle$ and towards this goal we define $L(K) = R^{\#}[K, K]^2 R^{\#}$ (here $R^{\#}$ denotes the ring R with 1 adjoined if necessary).

Lemma 9.1.4 $L(K) \subseteq \langle K \rangle$.

Proof. Let $a, b \in K$, $s \in S$. Then

$$(ab - ba)s = a(bs + sb) - (as + sa)b + (sab - bas) \in \langle K \rangle.$$

It follows that $[K, K]R^{\#} \subseteq \langle K \rangle$ (using $R = S + K$). Similarly $R^{\#}[K, K] \subseteq \langle K \rangle$ and the result is immediate.

It will also be useful to have the following description of $\langle K \rangle$ (valid for $*$ of either kind).

Lemma 9.1.5 $\langle K \rangle = K + K \circ K$.

Proof. For $a, b \in K$ we see from $2ab = [a, b] + a \circ b$ that $K^2 \subseteq K + K \circ K$. We note next that $K \circ K$ coincides with the additive subgroup generated by $\{a^2 \mid a \in K\}$. We now claim that $(K \circ K)K \subseteq K + K \circ K$. Indeed, for $a, b \in K$ we have $a^2b + ba^2 \in K$, $a^2b - ba^2 = a[a, b] + [a, b]a \in K \circ K$, whence $a^2b \in K + K \circ K$. From this we see that

$$K^3 = K^2K \subseteq (K + K \circ K)K \subseteq K^2 + (K \circ K)K \subseteq K + K \circ K$$

and, continuing in this fashion, we conclude that $K^n \subseteq K + K \circ K$ for any n. Since $\langle K \rangle = \sum K^n$, the lemma is proved.

We now define: for $U \lhd K$, $I_U = R^{\#}[U \circ U, U]^2 R^{\#}$. We shall call a Lie ideal U of K *exceptional* if $I_U = 0$.

Lemma 9.1.6 *If $U \lhd K$, then:*
(a) $I_U \subseteq \langle U \rangle$;
(b) $[I_U \cap K, K] \subseteq U$.

Proof. From

$$[a \circ b, x] = [a, x \circ b] + [b, a \circ x] = a \circ [b, x] + [a, x] \circ b$$

we infer that $[U \circ U, S] \subseteq U$ and $[U \circ U, K] \subseteq U \circ U$, whence $[U \circ U, R] \subseteq \langle U \rangle$. We then have

$$[U \circ U, U]R^{\#} \subseteq [U \circ U, UR^{\#}] + U[U \circ U, R^{\#}] \subseteq \langle U \rangle.$$

Similarly $R^{\#}[U \circ U, U] \subseteq \langle U \rangle$. Therefore $R^{\#}[U \circ U, U]^2 R^{\#} \subseteq \langle U \rangle$ and the result follows from Lemma 9.1.3 **(b)**.

Lemma 9.1.6 produces a standard Lie ideal I_U inside a Lie ideal U of K but the main problem arises when one tries to show (under appropriate circumstances) that $I_U \neq 0$. We shall deal with this problem by giving a complete description of what happens in the case $R = M_n(F)$, F an algebraically closed field, and then using GPI theory (i.e., Corollary 9.1.1) and the $*$-Litoff Theorem to reduce the general question to this very special case.

Theorem 9.1.7 *Let $R = M_n(F)$, $n \geq 2$, F an algebraically closed field of $char(F) \neq 2$, and let $*$ be an involution of the first kind on R. Then there is a set of matrix units in R relatively to which $*$ is either the transpose or symplectic involution, and K is a simple Lie algebra over F unless one of the following holds:*
(i) $n = 2$, $*$ is transpose (here K is 1-dimensional);
(ii) $n = 4$, $*$ is transpose (here K is the Lie direct sum $K_1 \oplus K_2$ where K_i, $i = 1, 2$, is a 3-dimensional simple Lie algebra).

Proof. By Corollary 4.6.13 $*$ is either the transpose involution or the symplectic involution relative to a suitable set of matrix units $\{e_{ij}\}$.

We first discuss the transpose case. We set $E_{ij} = e_{ij} - e_{ji}$, $i \neq j$, and note that $\{E_{ij} \mid i < j\}$ is a basis for K. For convenience if $x = \sum_{i<j} \alpha_{ij} E_{ij} \in K$ the "length" of x is the number of nonzero α_{ij}'s. The E_{ij} satisfy $E_{ij} = -E_{ji}$, $[E_{ij}, E_{jk}] = E_{ik}$, $i \neq k$, and the consequences thereof. Clearly $[K, K] = 0$ if and only if $n = 2$, and so we may assume that $n > 2$. Suppose $0 \neq U \triangleleft K$ and pick $0 \neq u = \sum \alpha_{ij} E_{ij} \in U$ of smallest length. If u is of the length 1, then it is easy to show that any basis element E_{kl} lies in U, whence $U = K$. If E_{ij}, E_{ik} appear in u for $j \neq k$, then $0 \neq [u, E_{ij}] \in U$ is of smaller length than u. Therefore we may assume that the E_{ij}'s appearing in u are "disjoint" and thus we may write u (say) as $\alpha E_{12} + \beta E_{34} + \gamma E_{56} + \ldots$. If the length of $u \geq 3$, then $[u, E_{45}] \neq 0$ is of smaller length than u, and so we may assume that the length of u is 2. This forces $n \geq 4$. If $n > 4$, then $[u, E_{45}] \neq 0$ has length 1, whence $U = K$. Therefore we are left with $n = 4$. Here it is well-known (and easy to show directly) that $K = K_1 \oplus K_2$, where K_1 and K_2 are both 3-dimensional simple Lie algebras with respective bases

$$\{E_{12}+E_{34}, E_{13}+E_{42}, E_{14}+E_{23}\}, \ \{E_{12}-E_{34}, E_{13}-E_{42}, E_{14}-E_{23}\}.$$

This completes the proof in the transpose case.

In the symplectic case $n = 2m$ is even and it is easily seen that K contains of all matrices of the form

$$\begin{pmatrix} A & S \\ T & -{}^tA \end{pmatrix}$$

where $A, S, T \in M_m(F)$, ${}^tA$ the transpose of A, and S, T belong the set H of symmetric elements of $M_m(F)$. Letting $\{e_{ij}\}$ be matrix units for $M_m(F)$ we note that $\{e_{ii}, e_{ij} + e_{ji}\}$, $i \neq j$, is a basis for H. The reader may verify (by easy matrix calculations) that H is a simple Jordan algebra. Now let $0 \neq U \lhd K$ and pick a nonzero element $u = \begin{pmatrix} A & S \\ T & -{}^tA \end{pmatrix} \in U$. If both $S \neq 0$ and $T \neq 0$ we may replace u by

$$\left[u, \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}\right] = \begin{pmatrix} -T & A + {}^tA \\ 0 & T \end{pmatrix}.$$

Thus we may assume $u = \begin{pmatrix} A & S \\ 0 & -{}^tA \end{pmatrix}$ to begin with and, if $A \neq 0$, we choose $P \in H$ such that $AP + P\,{}^tA \neq 0$ and note that

$$\left[u, \begin{pmatrix} 0 & P \\ 0 & 0 \end{pmatrix}\right] = \begin{pmatrix} 0 & AP + P\,{}^tA \\ 0 & 0 \end{pmatrix} \neq 0.$$

Thus we may assume that $u = \begin{pmatrix} 0 & S \\ 0 & 0 \end{pmatrix}$ for some $S \neq 0$. From

$$\left[\begin{pmatrix} T & 0 \\ 0 & -T \end{pmatrix}, \begin{pmatrix} 0 & S \\ 0 & 0 \end{pmatrix}\right] = \begin{pmatrix} 0 & TS + ST \\ 0 & 0 \end{pmatrix},$$

$T \in H$, it follows that $\left\{ S \in H \mid \begin{pmatrix} 0 & S \\ 0 & 0 \end{pmatrix} \right\}$ is a nonzero Jordan ideal of H and hence equal to H. Therefore U contains all matrices of the form $\begin{pmatrix} 0 & S \\ 0 & 0 \end{pmatrix}$, $S \in H$, and, by commutation with $\begin{pmatrix} 0 & 0 \\ I & 0 \end{pmatrix}$, all matrices of the form $\begin{pmatrix} 0 & 0 \\ T & 0 \end{pmatrix}$, $T \in H$. The calculation

$$\left[\begin{pmatrix} 0 & e_{ij} + e_{ji} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ e_{jj} & 0 \end{pmatrix}\right] = \begin{pmatrix} e_{ij} & 0 \\ 0 & -e_{ji} \end{pmatrix}$$

then shows that U contains all matrices of the form $\begin{pmatrix} A & 0 \\ 0 & -{}^tA \end{pmatrix}$, and the proof of the theorem is complete.

We now compile a set of remarks which follows almost immediately (with the help of an occasional matrix calculation) from Theorem 9.1.7.

Corollary 9.1.8 *Let $R = M_n(F)$ be as in Theorem 9.1.7 and let U, V denote Lie ideals of K. Then:*

(a) *$U = 0$ or $U = K$ unless $n = 4$, $*$ is transpose, in which case U may also be K_1 or K_2.*

(b) *The following are equivalent:*

(b1) *U is trivial;*

(b2) *$U = 0$ or $n = 2$, $*$ is transpose, in which case $U = K$ is 1-dimensional;*

(b3) *$[U, U]^2 = 0$;*

(c) *The following are equivalent:*

(c1) *U is exceptional;*

(c2) *$U \circ U$ is central;*

(c3) *U is trivial, $U = K_1$ or $U = K_2$ ($n = 4$, $*$ is transpose) or $U = K$ ($n = 2$, $*$ is transpose or symplectic);*

(d) *$[U, V] \equiv 0$ if and only if $U \equiv 0$, $V \equiv 0$, or (say) $U = K_1$ and $V = K_2$ ($n = 4$, $*$ is transpose).*

Now let R be an arbitrary prime ring with involution of the first kind, and let F be the algebraic closure of C. We form the extension $\tilde{R} = RC \otimes_C F$ which by Theorem 2.3.5 is a prime ring. We claim that $\tilde{R}$ is centrally closed over F. Indeed, letting $\tilde{C}$ denote the extended centroid of $\tilde{R}$, we note that the inclusion $F \subseteq \tilde{C}$ is obvious where F is identified with $1 \otimes F \subseteq Q_s(R) \otimes_C F$. Let $\alpha \in \tilde{C}$. By Theorem 2.3.5 there exist nonzero elements $a \in R$ and $f \in F$ such that $u = \alpha \cdot (a \otimes f) \in \tilde{R}$. Let $u = \sum_{i=1}^n a_i \otimes f_i$, $a_i \in R$, $f_i \in F$. Without loss of generality we can assume that $a_1, \ldots, a_n$ and $f_1, \ldots, f_n$ are two sets of C-independent elements. Then $u(x \otimes 1)(a \otimes f) = (a \otimes f)(x \otimes 1)u$ for every $x \in R$ and so $a_i x a = a x a_i$ for all $i = 1, 2, \ldots, n$. By Theorem 2.3.4 there exist $c_1, c_2, \ldots, c_n \in C$ such that $a_i = c_i a$, $i = 1, 2, \ldots, n$ and taking into account the C-independence of $a_1, a_2, \ldots, a_n$ we see that $n = 1$ and $\alpha \cdot (a \otimes c) = a_1 \otimes f_1 = (a \otimes f)(1 \otimes f^{-1} c_i f_i$ which proves our claim. Next the involution $*$ on R can clearly be lifted to an involution $*$ of the first kind on $\tilde{R}$ according to the rule $(rc \otimes \lambda)^* = r^* c \otimes \lambda$. The skew elements $\widetilde{K}$ of $\tilde{R}$ coincide with $KF = KC \otimes F$ and any Lie ideal U of K lifts to a Lie ideal $\tilde{U} = UC \otimes F = UF$ in $\widetilde{K}$. In case R is PI we can draw the following conclusion.

Theorem 9.1.9 *Let R be a prime PI-ring with involution $*$ of the first kind. Then:*

(a) *RC is finite dimensional central simple over C and $\tilde{R} = M_n(F)$, F the algebraic closure of C;*

(b) *KC is a simple Lie ring unless $n = 2$ ($*$ is transpose) or $n = 4$ ($*$ is transpose);*

(c) *If U is a nonzero exceptional Lie ideal of K then one of the following hold:*

(c1) *$n = 2$, $*$ is transpose, $\tilde{U} = \widetilde{K}$;*

(c2) *$n = 2$, $*$ is symplectic, $\tilde{U} = \widetilde{K}$;*

(c3) *$n = 4$, $*$ is transpose, $\tilde{U} = \widetilde{K}_1$ or $\tilde{U} = \widetilde{K}_2$.*

Proof. **(a)** is a consequence of Posner's Theorem. To prove **(b)** let $0 \neq U \lhd KC$. By Theorem 9.1.7 $\tilde{U} = \widetilde{K}$ unless $n = 2$ ($*$ is transpose) or $n = 4$ ($*$ is transpose). Let $a \in K$. Then $a \otimes 1 = \sum_{i=1}^{m} u_i \otimes \lambda_i$, $u_i \in U$, $\lambda_i \in F$ with $\{\lambda_i\}$ C-independent and $\lambda_1 = 1$. It follows that $a = u_1 \in U$ and so $U = KC$, thus proving **(b)**. Part **(c)** is an immediate application of Corollary 9.1.8 **(c)**.

As promised at the end of section 6.2 we are now in a position to deal with a conjecture made by Herstein in 1955: if R is a ring with involution and K is PI then R is PI. Herstein verified his own conjecture in 1967 [114] for R simple, and this was shortly thereafter extended to semiprime rings by Martindale [206] and then to arbitrary rings with involution by Amitsur

[6]. We present here an alternate proof for the case where R is prime.

Theorem 9.1.10 *Let R be a prime ring with involution $*$ (of either kind) and suppose K is PI (over C). Then R is PI.*

Proof. Without loss of generality we may assume that K satisfies a multilinear PI $\phi(x_1, x_2, \ldots, x_n) \in C{<}X{>}$ of degree n. If $*$ is of the second kind we choose a nonzero skew element λ in C and with it a nonzero $*$-ideal I such that $\lambda I \subseteq R$. Note that $I = I \cap S \oplus I \cap K$ and $\lambda(I \cap S) \subseteq K$. Therefore $\phi(r_1, \ldots, r_n) = 0$ where each r_i belongs to either $I \cap K$ or $\lambda(I \cap S)$. Since ϕ is multilinear it follows that $\phi(r_1, \ldots, r_n) = 0$ where each r_i belongs to either $I \cap K$ or $I \cap S$ and so ϕ is a PI on I. By Theorem 6.4.4 ϕ is then a PI on R.

We may therefore assume that $*$ is of the first kind, and furthermore, without loss of generality, we may suppose that $R = \tilde{R}$ (since ϕ lifts to $\widetilde{K}$). By Corollary 9.1.1 R is a centrally closed GPI algebra over an algebraically closed field F, whence R has nonzero socle H and associated division ring F. If R is not PI the dimension of the underlying vector space over F is infinite and so by the $*$-Litoff Theorem R contains $eRe \cong M_k(F)$, e a symmetric idempotent of finite rank $k \geq 2n$. By Corollary 4.6.13 the involution $*$ induced on $M_k(F)$ is either the transpose or symplectic involution. If $*$ is transpose then

$$\phi(e_{12} - e_{21}, e_{23} - e_{32}, \ldots, e_{n,n+1} - e_{n+1,n}) = \alpha e_{1,n+1} + \beta e_{n+1,1}$$

produces a contradiction. If $*$ is symplectic, then writing $k = 2m$ and letting $\{e_{ij}\}$ denote the matrix units in $M_m(F)$, we write

$$\begin{aligned} a_i &= \begin{pmatrix} e_{i,i+1} & 0 \\ 0 & -e_{i+1,i} \end{pmatrix}, \quad i = 1, 2, \ldots, n-1, \\ a_n &= \begin{pmatrix} e_{n,1} & 0 \\ 0 & -e_{1,n} \end{pmatrix}, \end{aligned}$$

$$b_i = \begin{pmatrix} e_{ii} & 0 \\ 0 & -e_{ii} \end{pmatrix}, \quad i = 1, 2, \ldots, n.$$

We then arrive at the contradiction

$$0 = \phi(a_1, a_2, \ldots, a_n) = \sum \alpha_i b_i, \quad \alpha_i \in C$$

some $\alpha_i \neq 0$. Therefore R must be PI and the theorem is proved.

Returning to the assumption that R is prime with involution $*$ of the first kind, we now approach the heart of this section. First, however, we need

Lemma 9.1.11 *If* $0 \neq I$ *is a* $*$ *ideal of* R *and* $0 \not\equiv U \triangleleft K$, *then* $[I \cap K, U] \not\equiv 0$.

Proof. Suppose $[I \cap K, U] \equiv 0$. Then, writing $[I \cap K, I \cap K] = (I \cap K)^{(1)}$ and using the Jacobi identity, we have $[(I \cap K)^{(1)}, U] = 0$, whence $[\langle (I \cap K)^{(1)} \rangle, U] = 0$. Thus $\langle (I \cap K)^{(1)} \rangle$ cannot contain a nonzero ideal of R and so by Lemma 9.1.6**(a)**

$$[(I \cap K)^{(1)} \circ (I \cap K)^{(1)}, I \cap K]^2 = 0.$$

By Theorem 9.1.10 (applied to the prime ring I) we conclude that I is PI, whence by Theorem 6.4.4 R is PI. In this situation we know that $\widetilde{R} = M_n(F)$. It follows that $\widetilde{I} = \widetilde{R}$ and accordingly $\widetilde{I \cap K} = \widetilde{K}$. Therefore our original supposition forces $[\widetilde{K}, \widetilde{U}] \equiv 0$, a contradiction to Corollary 9.1.8**(d)**.

Theorem 9.1.12 *If* R *is a prime ring with involution of the first kind and* $0 \neq U$ *is an exceptional Lie ideal of* K, *then* R *is* PI *(whence the conclusion of theorem 9.1.9 holds).*

Proof. We suppose R is not PI. Since $0 \neq \widetilde{U}$ is clearly an exceptional Lie ideal of $\widetilde{K}$ we may assume without loss of generality that $R = \tilde{R}$. Assume first that R has nonzero socle H. If $[H \cap K, H \cap K]^2 = 0$, then by Theorem 9.1.10 (applied to H) H, and hence R, is PI. Therefore we can suppose that $[H \cap K, H \cap K]^2 \neq 0$. Then $J = H[H \cap K, H \cap K]^2 H$ is a nonzero ideal of H (and hence of R) which by Lemma 9.1.4 is contained in $\langle H \cap K \rangle$. It follows that $0 \neq [U, H \cap K] \subseteq U \cap H$. Choosing $0 \neq u \in U \cap H$ we apply the $*$-Litoff Theorem to find a symmetric idempotent $e \in H$ such that $u \in eRe \cong M_m(F)$ where $m > 4$. Thus $U \cap eRe$ is a nonzero exceptional ideal of eKe is eRe, a contradiction to theorem 9.1.9.

We now suppose R has zero socle. If for all $u \in U$, $1, u, u^2$ are F-dependent, it follows that $u^2 = \beta \in F$. Pick $0 \neq a \in U$ (necessarily $a \notin F$). For all $k, l \in K$ we have $[[a, k]^2, l] = 0$ and so $\phi(x_1, x_2) = [[a, x_1]^2, x_2]$ is a nontrivial GPI for K over F. But by Corollary 6.2.5 this forces R to be GPI and hence have nonzero socle. Therefore we must conclude that there exists $a \in U$ such that $1, a, a^2$ are F-independent. Since U is exceptional, we see from $[U \circ U, U]^2 = 0$ that

$$[[a, k_1]^2, [a, k_2]][[a, k_3]^2, [a, k_4]] = 0 \quad \text{for all } k_1, k_2, k_3, k_4 \in K.$$

Since $1, a, a^2$ are F-independent, one sees that

$$f(x_1, x_2, x_3, x_4) = [[a, x_1]^2, [a, x_2]][[a, x_3]^2, [a, x_4]]$$

is a nontrivial GPI for K over F, again forcing the contradiction that the socle of R is nonzero in view of Corollary 6.2.5. The proof of the theorem is now complete.

We come now to the main result of this section.

Theorem 9.1.13 *Let R be a prime ring with involution $*$ of the first kind and let U, V be Lie ideals of K. Then:*

(a) If $U \equiv 0$, then $U = 0$ or $\tilde{R} = M_2(F)$ ($*$ is transpose, $\tilde{U} = \tilde{K}$ is 1-dimensional);

(b) *If U is exceptional, then $U \equiv 0$, $\tilde{R} = M_2(F)$ ($*$ is symplectic, $\tilde{U} = \widetilde{K}$), or $\tilde{R} = M_4(F)$ ($*$ is transpose, $\tilde{U} = \widetilde{K}_1$ or $\tilde{U} = \widetilde{K}_2$);*

(c) *If U is not exceptional, then $0 \neq I_U \subseteq \langle U \rangle$ and $0 \not\equiv [I_U \cap K, K] \subseteq U$;*

(d) *If $[U,U]^2 = 0$, then $U \equiv 0$;*

(e) *If $[U,V] \equiv 0$, then $U \equiv 0$, $V \equiv 0$, or $\tilde{R} = M_4(F)$ ($*$ is transpose and (say) $\tilde{U} = \widetilde{K}_1$, $\tilde{V} = \widetilde{K}_2$).*

Proof. to prove **(a)** and **(b)** we see from Theorem 9.1.12 that R is PI, whence the conclusions follow from Corollary 9.1.8 ((**b**) and (**c**)). Part (**c**) is an immediate consequence of the definition of I_U and Lemma 9.1.6. To prove (**d**) and (**e**), in view of Corollary 9.1.8 ((**b**) and (**d**)) it suffices to show that R is PI. BY Theorem 9.1.12 we may assume that neither U nor V is exceptional. Then from part (**c**) together with Theorem 9.1.10 we see that I_U and $I_U \cap I_V$ are prime PI rings, whence R is PI.

The import of Theorem 9.1.13 is that except for a couple of low-dimensional cases every Lie ideal of K contains a nontrivial standard Lie ideal, $\langle K \rangle$ is "large" in the sense that it contains a nonzero ideal of R, and K itself is a "prime" Lie ring in the sense that the Lie product of any two nonzero Lie ideals cannot be 0.

The Jordan theory of prime rings (without and with involution) is a considerably easier affair than the Lie structure (see, e.g. [116] and [118]), but we shall forego these matter with the exception of one isolated result (not presented in its full generality) which will be needed in section 9.4.

Lemma 9.1.14 *Let R be a prime ring with involution of the first kind such that $\dim_C(RC) > 16$, and let S denote the set of symmetric elements of R. Then $\langle S \rangle$ contains a nonzero ideal of R, namely, $R^\#[S,S]R^\#$.*

Proof. From $[[s,t],k] = [[s,k],t] + [s,[t,k]]$ and $[s,k],[t,k] \in S$ for all $s,t \in S$, $k \in K$, it is clear that $[S,S]$ is a Lie ideal of K. If $[S,S] = 0$, then K is PI (it satisfies $[x^2, y^2] = 0$) and by Theorem 9.1.10 R is PI. In this situation it is easy to see that $\tilde{R}$ must be $M_2(F)$ under symplectic involution since $[\tilde{S},\tilde{S}] = 0$. Since this case is ruled out by the hypothesis, we conclude that $[S,S] \neq 0$. Since $\dim_C(RC) > 16$, we see by Theorem 9.1.13(c) there is an ideal $I \neq 0$ such that $I \subseteq \langle [S,S] \rangle \subseteq \langle S \rangle$.

9.2 The Lie Extended Centroid of K

We continue with our assumption that R is a prime ring with involution of the first kind. Our aim here is to show that, with the exception of certain low dimensional cases, the Lie extended centroid of K (which we shall presently define) coincides with the extended centroid C of R. Theorem 9.1.13(e) shows that K is (usually) a "prime" Lie ring and thus suggests that we make a brief digression into general nonassociative rings (see [101] for complete discussion).

Let A be an arbitrary nonassociative ring (i.e., all the ring axioms except for the associative law) with composition denoted by $a \cdot b$, $a, b \in A$. We say that A is *prime* in case $U \cdot V =$ implies $U = 0$ or $V = 0$ for any ideals U, V of A. The *centroid* Φ of A is by definition the set of all endomorphisms of $(A, +)$ which commute with all the left and right multiplications of A. It is a straightforward exercise ([101, Theorem 1.1(a)]) to show that Φ is a commutative integral domain with 1 and that A is Φ-torsion free provided A is prime. In the remainder of this digression we shall assume that A is a prime nonassociative ring and shall restrict ourselves to ideals which are Φ-invariant (i.e., A is a prime Φ-algebra). The *multiplication ring* $M(A)$ of A is the subring of $End_Z(A)$ generated by all the left and right multiplications of A, where $\mathcal{Z}$ is the ring of integers. We proceed to define the *extended centroid* of A. We begin by noting that the set $\mathcal{F}$ of all nonzero ideals of A is closed under finite intersections. For $U \in \mathcal{F}$ a Φ-map $f : U \to A$ is called *permissible* if f commutes with the elements of $M(A)$. Such an element will be denoted by (f, U). $\ker(f) = \{u \in U \mid f(u) = 0\}$ and $Im(f) = \{f(u) \mid u \in U\}$ are ideals of A and we note that $(\ker(f)) \cdot (Im(f)) = 0$. Hence by the primeness of A either $f = 0$ or f is an injection. We define $(f, U) \sim (g, V)$ if there exists $W \in \mathcal{F}$ such that $W \subseteq U \cap V$ and $f = g$ on W. This is easily shown to be an equivalence relation. We remark that $(f, U) \sim (g, V)$ if and only if there exists $0 \neq x \in U \cap V$ such that $f(x) = g(x)$. We denote by $[f, U]$ the equivalence class determined by (f, U) and let $C(A)$ be the set of all equivalence classes. Addition in $C(A)$ is defined by

$$[f, U] + [g, V] = [f + g, U \cap V]$$

and it is easy to check that this definition is independent of the representatives.

For (g, V) permissible and $U \in \mathcal{F}$, let $g^{-1}(U) = \{v \in V \mid g(v) \in U\}$. Clearly $g^{-1}(U)$ is an ideal of A and we show that it is nonzero. If $g(V) = 0$, then $0 \neq V \subseteq g^{-1}(U)$. If $g(V) \neq 0$, then $g(V) \cap U \neq 0$. Pick $v \in V$ such that $0 \neq g(v) \in U$. Hence $v \neq 0$ and $v \in g^{-1}(U)$. Now define multiplication in $C(A)$ by

$$[f, U][g, V] = [fg, g^{-1}(U)].$$

To see that multiplication is well-defined, suppose $(f_1, U_1) \sim (f_2, U_2)$ and $(g_1, V_1) \sim (g_2, V_2)$. Then $f_1 = f_2$ on $W_1 \subseteq U_1 \cap U_2$ and $g_1 = g_2$ on $W_2 \subseteq V_1 \cap V_2$. Set $W = W_2 \cap g^{-1}(W_1)$. For all $x \in W$,

$$f_1(g_1(x)) = f_1(g_2(x)) = f_2(g_2(x))$$

and so multiplication is well-defined. It is then straightforward to check that $C(A)$ is an associative ring with 1. We shall call $C(A)$ the *extended centroid* of A.

Theorem 9.2.1 *The extended centroid $C(A)$ of a prime nonassociative ring is a field.*

Proof. We first show that $C(A)$ is commutative. Let $\lambda = [f, U]$, $\mu = [g, V] \in C(A)$. We set $W = g^{-1}(U) \cap f^{-1}(V)$ and pick $x, y \in W$. Then

$$fg(xy) = f(g(x)y) = g(x)f(y) = g(xf(y)) = gf(xy).$$

It follows that $(fg - gf)(W)W = 0$, and so $(fg - gf)(W) = 0$, whence $\lambda\mu = \mu\lambda$. Next let $[f, U] \neq 0$ and note that $f(U) \neq 0$ but $\ker(f) = 0$. Define $g : f(U) \to A$ by $g(f(u)) = u$ for all $u \in U$. g is well-defined since f is an injection and in fact $(g, f(U))$ is permissible. Clearly $[g, f(U)]$ is the inverse of $[f, U]$, and the theorem is proved.

This completes our digression and we return to our assumption that R is a prime (associative) ring with involution of the first kind. We will also make the assumption that $\dim_C(RC) > 16$ (this will suffice for our purpose in section 9.4). We are therefore assured by Theorem 9.1.13(**e**) that K is a prime Lie ring, and so K has an extended centroid $\Gamma = C(K)$. Clearly $\Gamma \supseteq C = C(R)$. As a first step in showing that $\Gamma = C$ it will be useful to have the following

Lemma 9.2.2 *Let R be a simple GPI ring with involution $*$ of the first kind such that $\dim_C(RC) > 16$. Then K is a simple Lie ring.*

Proof. By Theorem 6.1.6 R is its own socle, and by Theorem 9.1.9(**b**) we may assume without loss of generality that R is not PI. Let $a, b \in K$, with $a \neq 0$. By the $*$-Litoff Theorem there exists a symmetric idempotent e in R such that $\dim_C(eRe) > 16$ and $a, b \in eRe$. Another application of Theorem 9.1.9(**b**), this time to the simple ring eRe, shows that eKe is a simple Lie ring. In particular b lies in the Lie ideal generated by a, and so we may conclude that K is a simple Lie ring.

Lemma 9.2.3 *If R is a centrally closed prime ring with involution $*$ of the first kind and* $\dim_C(R) > 16$, *then* $\Gamma = C$.

Proof. We assume first that R is not GPI. Let $\lambda = [f, U] \in \Gamma$, pick $0 \neq a \in U$, and set $b = f(a) \in K$. For $k \in K$ we see from the fact that (f, U) is permissible that

$$\begin{aligned}[][[b,k],[a,k]] &= [[f(a),k],[a,k]] = [f[a,k],[a,k]] \\ &= f[[a,k],[a,k]] = f(0) = 0.\end{aligned}$$

Thus $\phi(x) = [[b,x],[a,x]] \in R_C{<}X{>}$ is a GPI on K and so by Corollary 6.2.5 $\phi(x)$ must be the zero element of $R_C{<}X{>}$, forcing a and b to be C-dependent. Hence $b = \alpha a$ for some $\alpha \in C$. It follows that $\lambda = \alpha$ and so in the non-GPI case we have shown that $C = \Gamma$.

We now assume that R is GPI. In view of Theorem 6.1.6 R has nonzero socle H. We know that H is a simple GPI ring with involution of the first kind, centrally closed over C, and with $\dim_C(H) > 16$. By Lemma 9.2.2 (applied to H) we see that $K_H = K \cap H$ is a simple Lie ring. Furthermore we claim that $\Gamma = C(K_H)$. Indeed, if $\lambda = [f, U] \in \Gamma$ we know from $\dim_C(H) > 16$ and Theorem 9.1.13(**c**) that $[H \cap K, K] \subseteq U$ and hence $K_H = [H \cap K, K] \subseteq U$. Since $K_H = [K_H, K_H]$, we also see that $f(K_H) \subseteq K_H$. Our claim is therefore established, and it follows that $\lambda = [f, U]$ may be written $\lambda = [f, K_H]$. We now form the ring $S = H \otimes_C \Gamma$, which is a central simple GPI ring over Γ, with $\dim_\Gamma(S) > 16$, and with involution given by $h \otimes \lambda \mapsto h^* \otimes \lambda$. By Lemma 9.2.2 again (applied to S) we see that $K_H \otimes_C \Gamma$ is a simple Lie ring. We now define a mapping of $K_H \otimes_C \Gamma$ into K_H according to the rule

$$k \otimes \lambda \mapsto f(k), \quad k \in K_H,\ \lambda = [f, K_H] \in \Gamma.$$

In view of our previous remarks it is easily seen that this is a well-defined Lie homomorphism, and because of the Lie simplicity of $K_H \otimes \Gamma$, it is actually a Lie isomorphism. Now pick $\lambda = [f, K_H] \in \Gamma$ and $0 \neq a \in K_H$. Then $a \otimes \lambda - f(a) \otimes 1$ maps to $f(a) - f(a) = 0$, and so $a \otimes \lambda = f(a) \otimes 1$. This forces $\lambda \in C$ and completes the proof that $\Gamma = C$.

We now remove the assumption that R is centrally closed.

Theorem 9.2.4 *Let R be a prime ring with involution $*$ of the first kind such that* $\dim_C(RC) > 16$. *Then* $C(K) = C(R)$.

Proof. We have already pointed out that K is a prime Lie ring and that $C = C(R) \subseteq C(K)$. We claim that $C(K) \subseteq C(KC)$ via the mapping $[f, U] \mapsto [g, UC]$, where $g(\sum u_i c_i) = \sum f(u_i)c_i$. Indeed, the main thing to show is that g is well-defined. Suppose $\sum u_i c_i = 0$. Pick $v \in U$ and note that

$$\begin{aligned}\left[\sum f(u_i)c_i, v\right] &= \sum [f(u_i), v]c_i = \sum [u_i, f(v)]c_i \\ &= \left[\sum u_i c_i, f(v)\right] = 0.\end{aligned}$$

By the primeness of KC we infer that $\sum f(u_i)c_i = 0$, and from this it follows easily that the claim is established. By Lemma 9.2.3 we see that $C(KC) = C(RC)$, and so from

$$C(R) \subseteq C(K) \subseteq C(KC) = C(RC) = C(R)$$

we conclude that $C(R) = C(K)$.

9.3 Trilinear Symmetric Mappings

Let R be an algebra over a commutative ring Φ, and let V be a Φ-subspace of R. We shall say that a mapping $B : V^n \to R$ is *n-linear symmetric* if

(i) $B(x_1, x_2, \ldots, x_n) = B(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$ for all $x_1, x_2, \ldots, x_n \in V$ and all permutations $\sigma \in S_n$;

(ii) $B(x_1, \ldots, x_i + y_i, \ldots, x_n) = B(x_1, \ldots, x_i, \ldots, x_n)$ $+B(x_1, \ldots, y_i, \ldots, x_n)$ for all $i = 1, 2, \ldots, n$, $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots, y_n \in V$;

(iii) $B(x_1, \ldots, cx_i, \ldots, x_n) = cB(x_1, \ldots, x_i, \ldots, x_n)$ for all $i = 1, 2, \ldots, n$, $x_1, x_2, \ldots, x_n \in V$, $c \in \Phi$.

In case Φ is the ring of integers we shall say that B is n-additive symmetric. Consider then an n-linear symmetric mapping $B : V^n \to R$. The mapping $T : V \to R$ given by $T(x) = B(x, x, \ldots, x)$ is called the *trace* of B ; T is said to be *commuting* if $[T(x), x] = 0$ for all $x \in V$. This last condition shows that generalized identities arise quite naturally in the study of such mappings.

The simplest case, $V = R$ a prime ring and $n = 1$, goes back to 1957 when Posner [241] showed that the existence of a nonzero commuting derivation in a prime ring implied that R was commutative. A variety of results on commuting mappings have since been obtained by a number of authors (e.g. [224], P. H. Lee and T. K. Lee [173], [164], [39], [69], etc.). Many of these isolated results were simultaneously generalized in 1993 by Bresar [62], and we now proceed to present the details of his result in a series of easy steps (we shall need this result at one place in section 9.4).

Let R be a ring. A biadditive map $B : R \times R \to R$ is called a *biderivation* if for every $x \in R$ the map $y \mapsto B(x, y)$ is a derivation of R and for every $y \in R$ the map $x \mapsto B(x, y)$ is a derivation of R. The notion of biderivation arises naturally in the study of additive commuting maps, namely, the linearization

$$[f(x), y] = [x, f(y)] \tag{9.1}$$

of an additive commuting map f implies that the mapping $B : R \times R \to R$ given by $B(x, y) = [f(x), y]$ is a biderivation.

Lemma 9.3.1 *Let R be a ring and $B : R \times R \to R$ a biderivation. Then*

$$B(x,y)z[u,v] = [x,y]zB(u,v) \quad \textit{for all } x,y,z,u,v \in R.$$

Proof. We compute $B(xu, yv)$ in two different ways. Using the fact that B is a derivation in the first argument, we get

$$B(xu,yv) = B(x,yv)u + xB(u,yv). \tag{9.2}$$

Since B is a derivation in the second argument, it follows from (9.2) that

$$B(xu,yv) = B(x,y)vu + yB(x,v)u + xB(u,y)v + xyB(u,v).$$

Analogously, we obtain

$$\begin{aligned} B(xu,yv) &= B(xu,y)v + yB(xu,v) \\ &= B(x,y)uv + xB(u,y)v + yB(x,v)u + yxB(u,v). \end{aligned}$$

Comparing the relations so obtained for $B(xu, yv)$ we arrive at

$$B(x,y)[u,v] = [x,y]B(u,v) \quad \text{for all } x,y,u,v \in R.$$

Replacing u by zu and using the relations

$$[zu,v] = [z,v]u + z[u,v], \quad B(zu,v) = B(z,v)u + zB(u,v)$$

we obtain the assertion of the lemma.

We are now in a position to prove

Theorem 9.3.2 *Let R be a noncommutative prime ring and let $B : R \times R \to R$ be a biderivation. Then there exists $\lambda \in C$ such that $B(x,y) = \lambda[x,y]$ for all $x, y \in R$.*

Proof. Let $S = R \times R$ and define $A : S \to R$ by $A(x,y) = [x,y]$; $A \neq 0$ since R is noncommutative. By Lemma 9.3.1 the functions $A, B : S \to R$ satisfy all the requirements of Lemma 7.9.11. Hence the result follows.

As a consequence of Theorem 9.3.2 we obtain

Corollary 9.3.3 *Let R be a prime ring. If $f : R \to R$ is an additive commuting map, then there exists $\lambda \in C$ and an additive map $\mu : R \to C$ such that $f(x) = \lambda x + \mu(x)$ for all $x \in R$.*

Proof. Linearizing $[f(x), x] = 0$ we see that the map $(x, y) \mapsto [f(x), y]$ is a biderivation. Clearly we may assume R is noncommutative. Therefore by Theorem 9.3.2 there exists $\lambda \in C$ such that $[f(x), y] = [\lambda x, y]$ for all $x, y \in R$. Hence we see that for any $x \in R$ the element $\mu(x) = f(x) - \lambda x \in C$, and the proof is complete.

Bresar's characterization of biadditive symmetric mappings with commuting traces for $V = R$ a prime ring of $char(R) \neq 2$ [63] was a landmark achievement, for (along with a variety of applications) it enabled him to settle a long standing conjecture of Herstein ([113],) concerning Lie isomorphisms of prime rings. For us this work of Bresar served as the inspiration to attempt to characterize trilinear symmetric mappings with commuting traces for the situation where R is a prime ring with involution and $V = K$. It will be seen in section 9.4 how critical a role this characterization plays in the verification of Herstein's conjecture ([31, Theorem 3]) concerning Lie isomorphisms of the skew elements of a prime ring with involution. We now state the main result we wish to prove. The remainder of this section will be devoted to its proof.

Theorem 9.3.4 (Beidar, Martindale, Mikhalev [31]) *Let R be a centrally closed prime ring over C with involution $*$ of the first kind, and with $char(R) \neq 2, 3$. Furthermore assume that R is not GPI. Let $B : K^3 \to K$ be a trilinear symmetric mapping whose trace T is commuting. Then there exist $\lambda \in C$ and a bilinear mapping $\mu : K \times K \to C$ such that*

$$\begin{aligned} 6B(x, y, z) &= \lambda(xyz + xzy + yxz + yzx + zxy + zyx) \\ &\quad + \mu(y, z)x + \mu(x, z)y + \mu(x, y)z \end{aligned}$$

for all $x, y, z \in K$.

The Proof of Theorem 9.3.4 will follow from a series of observations and lemmas. Throughout the conditions of the theorem will be assumed. We also caution the reader of a slight change of notation (both here and in section 9.4): small letters $x, y, \ldots$ will be elements of R and capital letters $X, Y, \ldots$ will denote variables.

We begin by linearizing our given condition

$$[B(x,x,x),x] = 0 \quad x \in K \tag{9.3}$$

through various stages. By replacing x by $x+y$ in (9.3) we are led to

$$\begin{aligned}[B(x,x,x),y] &+ 3[B(x,x,y),x] + 3[B(x,x,y),y]\\ &+ 3[B(x,y,y),x] + 3[B(x,y,y),y]\\ &+ [B(y,y,y),x] = 0\end{aligned} \tag{9.4}$$

Replacing y by $-y$ and y by $2y$ in (9.4) we obtain

$$[B(x,x,x),y] + 3[B(x,x,y),x] = 0,$$

i.e.,

$$[B(x,x,y),x] = -\frac{1}{3}[B(x,x,x),y] \tag{9.5}$$

and

$$[B(x,x,y),y] = -[B(x,y,y),x] \tag{9.6}$$

Substitution of x by $x+z$ in (9.5) the results in

$$2[B(x,y,z),x] + [B(x,x,y),z] + [B(x,x,z),y] = 0 \tag{9.7}$$

and finally replacement of x by $x+u$ in (9.7) leads to

$$\begin{aligned}[B(x,y,z),u] + [B(x,y,u),z] &+ [B(x,z,u),y]\\ &+ [B(y,z,u),x] = 0\end{aligned} \tag{9.8}$$

for all $x, y, z, u \in K$.

Before proceeding to our first lemma it will be convenient to define

$$\phi_{x,i}(y) = x^i y + x^{i-1}yx + \ldots + yx^i, \quad x, y \in R, \ i = 0, 1, 2, \ldots$$

(it is understood that $\phi_{x,0}(y) = y$) and then to immediately note that

$$\phi_{x,i}[y, x] = [y, x^{i+1}] \tag{9.9}$$

Lemma 9.3.5 *If $x \in K$ is algebraic over C of degree $m + 1$, then*

$$B(x, x, x) = \sum_{i=0}^{m} \beta_i x^i, \quad \beta_i \in C, \ i = 0, 1, \ldots, m.$$

Proof. We set $b = B(x, x, y)$, $y \in K$, $a = B(x, x, x)$, noting from (9.5) that $[b, x] = -\frac{1}{3}[a, y]$. From (9.9) we have $\phi_{x,i}[b, x] = [b, x^{i+1}]$, $i = 0, 1, 2, \ldots$. Writing $\sum_{i=0}^{m+1} \alpha_i x^i = 0$, $\alpha_i \in C$, $\alpha_{m+1} = 1$, we see that

$$\sum_{i=0}^{m} \alpha_{i+1}\phi_{x,i}[b, x] = \left[b, \sum_{i=0}^{m} \alpha_{i+1}x^{i+1}\right] = \left[b, \sum_{j=0}^{m+1} \alpha_j x^j\right] = 0,$$

whence $\sum_{i=0}^{m} \alpha_{i+1}\phi_{x,i}[a, y] = 0$ for all $y \in K$. By Corollary 6.2.5 the element $f(Y) = \sum_{i=0}^{m} \alpha_{i+1}\phi_{x,i}[b, Y]$ must be the zero element of R_C<X>. This means in particular that

$$\sum_{i=0}^{m} \alpha_{i+1}\phi_{x,i}[a, y] = 0 \tag{9.10}$$

for all $y \in R$. With the help of Theorem 2.3.6, equation (9.10) may be translated into the tensor product equation

$$\sum_{i=0}^{m} \alpha_{i+1} \sum_{j=0}^{i} (x^{i-j} \otimes x^j)(a \otimes 1 - 1 \otimes a) = 0 \tag{9.11}$$

Reversing the summation and rewriting (9.11) we have

$$\sum_{j=0}^{m}\left\{\sum_{j\leq i\leq m}\alpha_{i+1}x^{i-j}a\right\}\otimes x^{j}-\sum_{j=0}^{m}\left\{\sum_{j\leq i\leq m}\alpha_{i+1}x^{i-j}\right\}\otimes ax^{j}=0 \tag{9.12}$$

For each summand of the tensor product in (9.12) let us agree to call the factor to the left of the tensor sign the coefficient of the factor to the right of the tensor sign. From our assumption that x is algebraic of degree $m+1$ we know that $1, x, \ldots, x^m$ are C-independent. Suppose (to the contrary of what we are trying to prove) that $1, x, \ldots, x^m, a$ are C-independent. We make the important observation that the coefficient of a in (9.12) is $\sum_{i=0}^{m}\alpha_{i+1}x^i = x^m + \sum_{i=0}^{m-1}\alpha_{i+1}x^i$, a polynomial in x of degree m. For $j > 0$, if ax^j is a linear combination of $1, x, \ldots, x^m, a, ax, \ldots, ax^{j-1}$ we rewrite (9.12) accordingly and note that the coefficient of a in the rewritten form of (9.12) remains a polynomial in x of degree m. A contradiction to $1, x, \ldots, x^m, a$ being independent is thereby reached, and so we may finally conclude that $a = B(x, x, x) = \sum_{i=0}^{m}\beta_i x^i$, $\beta_i \in C$.

Lemma 9.3.6 *If $z \in K$ is not algebraic of degree ≤ 6, then*

$$B(z,z,z) = \alpha z^5 + \beta z^3 + \gamma z, \quad \alpha, \beta, \gamma \in C.$$

Proof. Replacing x by z^3 in (9.7) we have

$$2[B(z^3,y,z),z^3] + [B(z^3,z^3,y),z] + [B(z^3,z^3,z),y] = 0 \tag{9.13}$$

for all $y \in K$. Applying (9.9) to the first summand of (9.13) we obtain

$$\phi_{z,2}2[B(z^3,y,z),z] + [B(z^3,z^3,y,z),z] + [B(z^3,z^3,z),y] = 0$$

which in view of (9.7) again may be rewritten as

$$\begin{aligned}&-\phi_{z,2}[B(z,z,z^3),y] - \phi_{z,2}[B(z,z,y),z^3]\\&+[B(z^3,z^3,y),z] + [B(z^3,z^3,z),y] = 0\end{aligned} \tag{9.14}$$

Using (9.9) in connection with the second summand in (9.14) we then have

$$\begin{aligned} &-\phi_{z,2}[B(z,z,z^3),y]-\phi_{z,2}^2[B(z,z,y),z]\\ &+[B(z^3,z^3,y),z]+[B(z^3,z^3,z),y]=0 \end{aligned} \tag{9.15}$$

An application of (9.5) to the second summand of (9.15) results in

$$\begin{aligned} &-\phi_{z,2}[B(z,z,z^3),y]+\frac{1}{3}\phi_{z,2}^2[B(z,z,z),y]\\ &+[B(z^3,z^3,y),z]+[B(z^3,z^3,z),y]=0 \end{aligned} \tag{9.16}$$

We then apply $\phi_{z,2}$ to (9.16) and use (9.9) to obtain

$$\begin{aligned} &-\phi_{z,2}^2[B(z,z,z^3),y]+\frac{1}{3}\phi_{z,2}^3[B(z,z,z),y]\\ &+[B(z^3,z^3,y),z^3]+\phi_{z,2}[B(z^3,z^3,z),y]=0 \end{aligned} \tag{9.17}$$

Using (9.5) on the third summand of (9.17) we have

$$\begin{aligned} &-\phi_{z,2}^2[B(z,z,z^3),y]+\frac{1}{3}\phi_{z,2}^3[B(z,z,z),y]\\ &-\frac{1}{3}[B(z^3,z^3,z^3),y]+\phi_{z,2}[B(z^3,z^3,z),y]=0 \end{aligned} \tag{9.18}$$

Multiplication of (9.18) by -3 and rearrangement of terms yields

$$\begin{aligned} &[B(z^3,z^3,z^3),y]-3\phi_{z,2}[B(z^3,z^3,z),y]\\ &+3\phi_{z,2}^2[B(z,z,z^3),y]-\phi_{z,2}^3[B(z,z,z),y]=0 \end{aligned} \tag{9.19}$$

For simplification of notation we rewrite (9.19) as

$$[d,y]-3\phi_{z,2}[c,y]+3\phi_{z,2}^2[b,y]-\phi_{z,2}^3[a,y]=0,\quad y\in K \tag{9.20}$$

where $a=B(z,z,z)$, $b=B(z^3,z,z)$, $c=B(z^3,z^3,z)$, and $d=B(z^3,z^3,z^3)$. By Corollary 6.2.5

$$f(Y)=[d,Y]-3\phi_{z,2}[c,Y]+3\phi_{z,2}^2[b,Y]-\phi_{z,2}^3[a,Y]$$

must be the zero element of $R_C{<}X{>}$ and so in particular

$$[d, y] - 3\phi_{z,2}[c, y] + 3\phi_{z,2}^2[b, y] - \phi_{z,2}^3[a, y] = 0 \tag{9.21}$$

for all $y \in R$. Using Theorem 2.3.6 we may translate (9.21) into the tensor product equation

$$\begin{aligned} &d \otimes 1 - 1 \otimes d - 3(z^2 \otimes 1 + z \otimes z + 1 \otimes z^2)(c \otimes 1 - 1 \otimes c) \\ &+ 3(z^2 \otimes 1 + z \otimes z + 1 \otimes z^2)^2(b \otimes 1 - 1 \otimes b) \\ &- (z^2 \otimes 1 + z \otimes z + 1 \otimes z^2)^3(c \otimes 1 - 1 \otimes c) \end{aligned} \tag{9.22}$$

Two side calculations yield

$$\begin{aligned} (z^2 \otimes 1 + z \otimes z + 1 \otimes z^2)^2 &= z^4 \otimes 1 + 2z^3 \otimes z + 3z^2 \otimes z^2 \\ &\quad +2z \otimes z^3 + 1 \otimes z^4 \qquad (9.23) \\ (z^2 \otimes 1 + z \otimes z + 1 \otimes z^2)^3 &= z^6 + 3z^5 \otimes z + 6z^4 \otimes z^2 \\ &\quad +7z^3 \otimes z^3 + 6z^2 \otimes z^4 \\ &\quad +3z \otimes z^5 + 1 \otimes z^6 \qquad (9.24) \end{aligned}$$

Inserting (9.23) and (9.24) in (9.22) and then expanding in full we see that

$$\begin{aligned} &d \otimes 1 - 1 \otimes d - 3\{z^2c \otimes 1 + zc \otimes +c \otimes z^2 \\ &-z^2 \otimes c - z \otimes cz - 1 \otimes cz^2\} \\ &+3\{z^4b \otimes 1 + 2z^3b \otimes z + 3z^2b \otimes z^2 + 2zb \otimes z^3 + b \otimes z^4 \\ &-z^4 \otimes b - 2z^3 \otimes bz - 3z^2 \otimes bz^2 - 2z \otimes bz^3 - 1 \otimes bz^4\} \\ &-\{z^6a \otimes 1 + 3z^5a \otimes z + 6z^4a \otimes z^2 + 7z^3a \otimes z^3 \\ &+6z^2a \otimes z^4 + 3za \otimes z^5 + a \otimes z^6 \\ &-z^6 \otimes a - 3z^5 \otimes az - 6z^4 \otimes az^2 - 7z^3 \otimes az^3 \\ &-6z^2 \otimes az^4 - 3z \otimes az^5 - 1 \otimes az^6\} = 0 \end{aligned} \tag{9.25}$$

Systematically rearranging the terms of (9.25) we have

$$(d - 3z^2c + 3z^4b - z^6a) \otimes 1 + (-3zc + 6z^3b - 3z^5a) \otimes z$$

$$
\begin{aligned}
&+(-3c+9z^2b-6z^4a)\otimes z^2+(6zb-7z^3a)\otimes z^3\\
&+(3b-6z^2a)\otimes z^4-3za\otimes z^5-a\otimes z^6+z^6\otimes a\\
&+3z^5\otimes az+6z^4\otimes az^2+7z^3\otimes az^3\\
&+6z^2\otimes az^4+3z\otimes az^5+1\otimes az^6\\
&-3z^4\otimes b-6z^3\otimes bz-9z^2\otimes bz^2-6z\otimes bz^3-3\otimes bz^4\\
&+3z^2\otimes c+3z\otimes cz+3\otimes cz^2-1\otimes d=0 \qquad (9.26)
\end{aligned}
$$

Since z is not algebraic of degree ≤ 6, we may speak of the degree of polynomials in z whose powers of z do not exceed 6. We know that $1, z, \ldots, z^6$ are C-independent. Suppose (contrary to what we are trying to prove) that $1, z, \ldots, z^6, a$ are C-independent. In a similar fashion to the proof of Lemma 9.3.5 we note that the coefficient of a in (9.26) is z^6 whereas the coefficients of

$$az, az^2, \ldots, az^6, b, bz, \ldots, bz^4, c, cz, cz^2, d$$

in (9.26) are all polynomials in z of degree < 6. Consequently, writing if necessary any of the above elements as a linear combination of preceding elements and then rewriting (9.26) accordingly, it follows that the coefficient of a in the rewritten form of (9.26) remains a polynomial in z of degree 6. This a contradiction to $1, z, \ldots, z^6, a$ being assumed C-independent and so $a = B(z,z,z) = \sum_{i=0}^{6} \beta_i z^i$. Since $B(z,z,z)$ is skew we finally have $B(z,z,z) = \alpha z^5 + \beta z^3 + \gamma z$, $\alpha, \beta, \gamma \in C$, as desired.

Lemma 9.3.7 *If $z \in K$ is not algebraic of degree 6, then there exist $\lambda, \mu \in C$ such that $B(z,z,z) = \lambda z^3 + \mu z$.*

Proof. If z is algebraic of degree ≤ 5, then by Lemma 9.3.5 $B(z,z,z) = \sum_{i=0}^{m} \beta_i z^i$ for some $m \leq 4$. But $B(z,z,z)$ is skew and so $B(z,z,z) = \beta_3 z^3 + \beta_1 z$. Therefore we may assume that z is not algebraic of degree ≤ 6, because z is not algebraic of degree 6 by our assumption. In the free product $R_C{<}X{>}$ we consider the following sets of elements:

$\{M_i(z,Y) \mid i = 1,2,\ldots,n\}$, the set of all monomials of the form $z^{j_0}Y^{k_1}z^{j_1}\ldots Y^{k_s}z^{j_s}$, where $j_0 + j_1 + \ldots + j_s \leq 6$ and $k_1 + k_2 + \ldots + k_s \leq 6$,
$\{(Y+z)^i \mid i = 0,1,\ldots,6\}$,
$\{(Y-z)^i \mid i = 0,1,\ldots,6\}$.
Since $1, z, \ldots, z^6$ are C-independent, each of the above three sets is a C-independent subset of $R_C{<}X{>}$. By Lemma 6.1.8 there exists $x \in K$ such that each of the sets $\{M_i(z,x)\}$, $\{(x+z)^i\}$, and $\{(x-z)^i\}$ is a C-independent subset of R. We let V denote the C-span of the set $\{M_i(z,x)\}$. Since none of the elements $z, x, x+z, x-z$ are algebraic of degree ≤ 6, Lemma 9.3.6 implies that the traces $T(z), T(x), T(x+z), T(x-z)$ are all elements of V and in fact are of "degree" ≤ 5 in x and "degree" ≤ 5 in z. It then follows from the equations

$$\begin{aligned} T(x+z) &= T(x) + T(z) + 3B(x,x,z) + 3B(x,z,z), \\ T(x-z) &= T(x) - T(z) - 3B(x,x,z) + 3B(x,z,z) \end{aligned}$$

that $B(x,x,z)$ and $B(x,z,z)$ are also elements of V of degree ≤ 5 in both x and z. Using (9.5), we may then conclude from

$$[B(x,x,x),z] = -3[B(x,x,z),x]$$

that $B(x,x,z)$ is of degree 1 in z. Next, using (9.6), from

$$[B(x,x,z),z] = -[B(x,z,z),x]$$

we see that $B(x,z,z)$ is of degree ≤ 2 in z. As a result it follows from

$$B(x,z,z),z] = -\frac{1}{3}[B(z,z,z),x]$$

that $B(z,z,z)$ has degree ≤ 3 in z. Since $B(z,z,z)$ is skew we then have $B(z,z,z) = \lambda z^3 + \mu z$, $\lambda, \mu \in C$, as desired.

Lemma 9.3.8 *Suppose that $z \in K$ is algebraic of degree 6. Then there exist $\lambda, \mu \in C$ such that $B(z,z,z) = \lambda z^3 + \mu z$.*

Proof. In the free product $R_C{<}X{>}$ we consider the following five sets:

$\{M_i(z,Y) \mid i = 1,2,\ldots,n\}$, the set of all monomials of degree ≤ 6 in Y and of degree ≤ 5 in z,

$\{Y^i \mid i = 0,1,\ldots,6\}$ which is a subset of the first set,

$\{(Y-z)^i \mid i = 0,1,\ldots,6\}$,

$\{(Y+z)^i \mid i = 0,1,\ldots,6\}$,

$\{(Y+2z)^i \mid i = 0,1,\ldots,6\}$.

Each of these sets is a C-independent subset of $R_C{<}X{>}$, so by Lemma 6.1.8 there exists $x \in K$ such that each of the five sets $\{M_i(z,x)\}$, $\{x^i\}$, $\{(x-z)^i\}$, $\{(x+z)^i\}$, and $\{(x+2z)^i\}$ is an independent subset of R. We let W denote the C-span of the set $\{M_i(z,x)\}$ and let W' denote the subspace of W whose elements are of degree ≤ 3 in x. Since none of the elements $x, x-z, x+z, x+2z$ are algebraic of degree 6, Lemma 9.3.7 implies that the traces $T(x), T(x-z), T(x+z), T(x+2z)$ all belong to W'. By adding the equations

$$\begin{aligned} T(x+z) &= T(x) + T(z) + 3B(x,x,z) + 3B(x,z,z) \\ T(x-z) &= T(x) - T(z) - 3B(x,x,z) + 3B(x,z,z) \end{aligned}$$

we have $6B(x,z,z) = T(x+z) + T(x-z) - 2T(x)$, and so $B(x,z,z) \in W'$. Next, from the equations

$$\begin{aligned} T(x+2z) &= T(x) + 8T(z) + 6B(x,x,z) + 12B(x,z,z) \\ 8T(x+z) &= 8T(x) + 8T(z) + 24B(x,x,z) + 24B(x,z,z) \end{aligned}$$

we obtain

$$8T(x+z) - T(x+2z) = 7T(x) + 18B(x,x,z) + 12B(x,z,z)$$

and so $B(x,x,z) \in W'$. In W we have the equation

$$[B(x,x,x),z] = -3[B(x,x,z),x]$$

from which we may conclude that $B(x,x,z)$ has degree 1 in z. We therefore see from

$$[B(x,x,z),z] = -[B(x,z,z,),x]$$

that $B(x,z,z)$ has degree ≤ 2 in z. Since z is algebraic of degree 6, we know from Lemma 9.3.5 that $B(z,z,z) = \sum_{i=0}^{5} \gamma_i z^i$, $\gamma_i \in C$, and so $[B(z,z,z),x] \in W'$. Therefore from the equation

$$[B(z,z,z),x] = -3[B(x,z,z),z]$$

we see that $B(z,z,z)$ is of degree ≤ 3 in z, and the proof of the lemma is complete.

Together Lemma 9.3.7 and Lemma 9.3.8 imply

Lemma 9.3.9 *For all $z \in K$ there exist $\lambda, \mu \in C$ such that $B(z,z,z) = \lambda z^3 + \mu z$.*

We next show that λ is independent of z.

Lemma 9.3.10 *There exists $\lambda \in C$ such that for all $z \in K$ $B(z,z,z) = \lambda z^3 + \mu(z)z$, $\mu(z) \in C$.*

Proof. Let a, b be any elements of K neither of which is algebraic of degree ≤ 3. In the free product $R_C{<}X{>}$ we consider two sets

$\{M_i(a,Y) \mid i = 1,2,\ldots,n\}$, the set of all monomials of degree ≤ 6 in Y and of degree ≤ 3 in a,

$\{M_i(b,Y) \mid i = 1,2,\ldots,n\}$, the set of all monomials of degree ≤ 6 in Y and of degree ≤ 3 in b

These are each C-independent subsets of $R_C{<}X{>}$ and so by Lemma 6.1.8 there exists $x \in K$ such that the sets $\{M_i(a,x)\}$ and $\{M_i(b,x)\}$ are both C-independent subsets of R. Let U denote the C-span of the set $\{M_i(a,x)\}$, and let U' denote the subspace of U where elements are of degree ≤ 3 in x. By

Lemma 9.3.9 $T(x), T(a), T(x+a), T(x-a)$ all belong to U' and so from the equations

$$\begin{aligned} T(x+a) &= T(x) + T(a) + 3B(x,x,a) + 3B(x,a,a) \\ T(x-a) &= T(x) - T(a) - 3B(x,x,a) + 3B(x,a,a) \end{aligned} \tag{9.27}$$

we conclude that $B(x,x,a)$ and $B(x,a,a)$ both lie in U'. From

$$[B(x,x,x),a] = -3[B(x,x,a),x]$$

we see that $B(x,x,a)$ is of degree 1 in a, whence from

$$[B(x,x,a),a] = -[B(x,a,a),x]$$

we see that $B(x,a,a)$ has degree ≤ 2 in a. Next from

$$[B(x,a,a),a] = -\frac{1}{3}[B(a,a,a),x]$$

we see that $B(x,a,a)$ has degree 1 in x, whence from

$$[B(x,x,x),a] = -[B(x,a,a),x]$$

we see that $B(x,x,a)$ has degree ≤ 2 in x. Returning to equation (9.27) and using Lemma 9.3.9 we write

$$\begin{aligned} \lambda_1(a+x)^3 + \mu_1(a+x) &= \lambda_2 a^3 + \mu_2 a + \lambda_3 x^3 \\ &\quad +\mu_3 x + 3B(x,x,a) \\ &\quad +B(x,a,a) \end{aligned} \tag{9.28}$$

for suitable $\lambda_i, \mu_i \in C$. Since the degrees of $B(x,x,a)$ and $B(x,a,a)$ in either x or in a do not exceed 2, we conclude from (9.28) that $\lambda_1 = \lambda_2$ and $\lambda_1 = \lambda_3$, whence $\lambda_2 = \lambda_3$. In a similar fashion, writing $B(b,b,b) = \lambda_2' b^3 + \mu_2' b$, our argument shows that $\lambda_2' = \lambda_3$ and therefore $\lambda_2 = \lambda_2' = \lambda$. In case $y \in K$ is algebraic of degree ≤ 3 we know by Lemma 9.3.5 that $B(y, y, y) = \mu y$, so, writing $y^3 = \gamma y$, we have

$$B(y, y, y) = \lambda y^3 + \mu y - \lambda y^3 = \lambda y^3 + (\mu - \gamma\lambda)y.$$

The proof of Lemma 9.3.10 is now complete.

Proof of Theorem 9.3.4. By Lemma 9.3.10 there exists $\lambda \in C$ such that

$$B(x, x, x) = \lambda x^3 + \gamma(x)x, \quad \gamma(x) \in C \tag{9.29}$$

for all $x \in K$. We proceed to linearize (9.29) in the usual fashion. Replacement of x by $x + y$ in (9.29) results in

$$3B(x, x, y)+3B(x, y, y) = \lambda(x^2y+xyx+yx^2+xy^2+yxy+y^2x)+h_1 \tag{9.30}$$

for all $x, y \in K$, where h_1 is a linear term in x and y. Replacement of y by $-y$ in (9.30) then quickly leads to

$$3B(x, y, y) = \lambda(xy^2 + yxy + y^2x) + h_2 \tag{9.31}$$

where h_2 is linear in x and y. Replacement of y by $y + z$ in (9.31) then results in

$$6B(x, y, z) = \lambda(xyz + xzy + yxz + yzx + zxy + zyx) + h \tag{9.32}$$

for all $x, y, z \in K$, where

$$h(x, y, z) = \alpha(x, y, z)x + \beta(x, y, z)y + \gamma(x, y, z)z \tag{9.33}$$

and $\alpha(x, y, z), \beta(x, y, z), \gamma(x, y, z) \in C$. We note from (9.32) that $h : K^3 \to K$ is a trilinear mapping. We define a mapping $\mu : K \times K \to C$ in the following fashion. Given $(y, z) \in K \times K$ choose $x \in K$ such that x does not lie in the C-span of y and z (such x exists since K is infinite dimensional over C). Now write

$$h(x, y, z) = \alpha x + \beta y + \gamma z$$

and define $\mu(y,z)=\alpha$. To show that μ is well-defined let $u \in K$ such that $u \notin Cy+Cz$. Suppose first that $u=\tau_1 x+\tau_2 y+\tau_3 z$ (necessarily $\tau_1 \neq 0$). Then

$$\begin{aligned}
h(u,y,z) &= \tau_1 h(x,y,z)+\tau_2(h(y,y,z)+\tau_3 h(z,y,z)\\
&= \tau_1(\alpha x+\beta y+\gamma z)+\tau_2(\beta_2 y+\gamma_2 z)+\tau_3(\beta_3 y+\gamma_3 z)\\
&= \alpha(\tau_1 x+\tau_2 y+\tau_3 z)+\beta_4 y+\gamma_4 z\\
&= \alpha u+\beta_4 y+\gamma_4 z
\end{aligned}$$

We may thus assume that u,x are C-independent modulo $Cy+Cz$. In this case we write

$$h(x,y,z)+h(u,y,z)=h(x+u,y,z)$$

whence

$$\alpha x+\beta y+\gamma z+\alpha_1 u+\beta_1 y+\gamma_1 z=\alpha_2(x+u)+\beta_2 y+\gamma_3 z \quad (9.34)$$

It follows from (9.34) that $\alpha=\alpha_2$ and $\alpha_1=\alpha_2$ and so $\alpha=\alpha_1$ as desired.

We next show that μ is bilinear. Let $y,y',z \in K$, $\tau \in C$, and choose $x \in K$ such that $x \notin Cy+Cy'+Cz$. The following equations

$$\begin{aligned}
h(x,y,z) &= \alpha x+\beta y+\gamma z=h(x,z,y)\\
h(x,y+y',z) &= \mu(y+y',z)x+\beta_1(y+y')+\gamma_1 z\\
&= h(x,y,z)+h(x,y'z)\\
&= \mu(y,z)x+\beta_2 y+\gamma_2 z+\mu(y',z)x+\beta_3 y'+\gamma_3 z\\
h(x,\tau y,z) &= \mu(\tau y,z)x+\beta_4\tau y+\gamma_4 z\\
\tau h(x,y,z) &= \tau\mu(y,z)x+\tau\beta y+\tau\gamma z
\end{aligned}$$

clearly imply that μ is bilinear.

Now let $x,y,z \in K$ be C-independent. From

$$\begin{aligned}
& h(x,y,z)=\mu(y,z)x+\beta y+\gamma z\\
=\ & h(y,x,z)=\mu(x,z)y+\beta_1 x+\gamma_1 z\\
=\ & h(z,x,y)=\mu(x,y)z+\beta_2 x+\gamma_2 y
\end{aligned}$$

we then conclude that

$$h(x, y, z) = \mu(y, z)x + \mu(x, z)y + \mu(x, y)z.$$

Next suppose that y, z are C-independent but $x \in Cy + Cz$. Choose $u \notin Cy + Cz$. Then $x + u \notin Cy + Cz$ and we have

$$\begin{aligned} h(x, y, z) &= h(x + u, y, z) - h(u, y, z) \\ &= \mu(y, z)(x + u) + \mu(x + u, z)y + \mu(x + u)z \\ &\quad -\mu(y, z)x - \mu(x, z)y - \mu(x, y)z \\ &= \mu(y, z)x + \mu(x, z)y + \mu(x, y)z \end{aligned} \tag{9.35}$$

Finally, if $\dim_C(Cx + Cy + Cz) = 1$, we choose $u \notin Cx + Cy + Cz$ and making use of the preceding case together with equation (9.35) we complete the proof of Theorem 9.3.4.

9.4 Lie Isomorphisms

At his 1961 AMS Hour Talk, entitled "Lie and Jordan structures in simple, associative rings", Herstein posed several problems he deemed worthy of attention [113]. Among these were the following questions (which we indicate in a rather loose fashion):

Problem 1. Is every Lie automorphism ϕ of a simple associative ring R given by (or "almost" given by) an automorphism σ or negative of an antiautomorphism σ of R?

Problem 2. If R is a simple ring with involution $*$ and K denotes the Lie ring of skew elements of R under $*$, is every Lie automorphism ϕ of K induced by (or "almost" induced by) an automorphism σ of R?

The qualification "almost" refers to the possibility that ϕ and σ may differ by an additive mapping τ of R into the center which sends commutators to 0.

The resolution of these problems in the classical case $R = M_n(F)$, F a field, has been well-known for a long time ([132, Chapter 10]). In 1951 Hua [130] solved Problem 1 for R a simple Artinian ring $M_n(D)$, D a division ring, $n \geq 3$. A more general situation for Problem 1 was subsequently considered by Martindale ([201], [203]) in which Lie isomorphisms $\phi : R \to R'$ (R, R' primitive in [201] and prime in [203]) were investigated and in which the matrix condition $n \geq 3$ was replaced by the condition that R contains three orthogonal idempotents whose sum is 1 (in [203] only two idempotents were required). A close look at the results of these papers reveals the fact that the image of σ in general requires a "larger" ring than R' and that the image of τ requires a "larger" field than the center of R'. We note that it was precisely this necessity to enlarge certain rings that was the motivation for developing the notions of extended centroid and central closure which proved so useful in characterizing prime GPI rings [205]. As mentioned in section 9.3, the final breakthrough on Problem 1 was made by Bresar [63]. Here, as a corollary to a general result on biadditive mappings in prime rings, he removed the assumption of orthogonal idempotents altogether and thereby settled Problem 1 in full generality.

Theorem 9.4.1 (Bresar [63, Theorem 3]) *Let R and R' be prime rings of characteristic $\neq 2$, neither of which satisfies the standard identity St_4. Then any Lie isomorphism ϕ of R onto R' is of the form $\phi = \sigma + \tau$, where σ is either an isomorphism or negative of an antiisomorphism of R into the central closure of R' and τ is an additive mapping of R into the extended centroid of R' sending commutators to* 0.

The present section is concerned with Problem 2. Let R be a prime ring with involution $*$, of characteristic $\neq 2, 3$, with K the skew elements of R, and C the extended centroid of R. Throughout this section all involutions will be of the first kind. (For involution of the second kind the feeling is that the solution of Problem 2 is inherently easier and should ultimately revert back to Theorem 9.4.1; partial results have been obtained by

M. P. Rosen [253]). As we have seen $*$ may be extended to an involution of the central closure RC according to $rc \mapsto r^*c$, $r \in R$, $c \in C$. Up to 1994 (see [31]) the main result concerning Problem 2 was the following theorem of Martindale [212], which we now state carefully since it plays a crucial role in the general solution of Problem 2.

Theorem 9.4.2 (Martindale [212, Theorem 3.1]) *Let R and R' be centrally closed prime rings of characteristic $\neq 2$ with involutions of the first kind, with algebraically closed centroids C and C' respectively, and with skew elements denoted respectively by K and K'. We assume furthermore that*

(a) $\dim_C(R) \neq 1, 4, 9, 16, 25, 64$;

(b) R contains two nonzero symmetric idempotents e_1 and e_2 such that $e_1 + e_2 \neq 1$;

(c) For $i = 1, 2$, $e_i \in \langle e_iRe_i \cap [K, K]\rangle$, the associative subring generated by $e_iRe_i \cap [K, K]$.

Then any Lie isomorphism of $[K, K]$ onto $[K', K']$ can be extended uniquely to an associative isomorphism of $\langle [K, K]\rangle$ onto $\langle [K', K']\rangle$.

Our aim in this section is to eliminate the requirement of idempotents assumed in Theorem 9.4.2. We are now ready to state the main result of this section:

Theorem 9.4.3 (Beidar, Martindale, Mikhalev [31]) *Let R and R' be prime rings with involutions of the first kind and of characteristic $\neq 2, 3$. Let K and K' denote respectively the skew elements of R and R' and let C and C' denote the extended centroids of R and R' respectively. Assume that* $\dim_C(RC) \neq 1, 4, 9, 16, 25, 64$. *Then any Lie isomorphism α of K onto K' can be extended uniquely to an associative isomorphism of $\langle K\rangle$ onto $\langle K'\rangle$, the associative subrings generated by K and K' respectively.*

It is interesting to note that the possibility of the mapping $\tau : R \to C'$ appearing in the conclusion of Theorem 9.4.3 does not in fact occur. We also mention that counterexamples illustrating the dimension restrictions on $\dim_C(RC)$ may be found in [212].

In view of Theorem 9.1.13 and Lemma 9.1.4 we have the following

Corollary 9.4.4 *If in Theorem 9.4.3 R and R' are simple rings, then α can be extended uniquely to an isomorphism of R onto R'.*

The proof of Theorem 9.4.3 is self-contained with a single major exception. Theorem 9.4.2 is required and in fact plays a decisive role; we refer the reader to [212] for the details of its proof. For the remainder of this section we shall assume that the conditions of the Theorem 9.4.3 hold. Our plan of attack is to consider two cases: Case A in which R is GPI and Case B in which R is not GPI. In Case A we are able to make use of Theorem 9.4.2. In case B we set up a certain trilinear symmetric mapping $B : K^3 \to K$ intimately related to α. Then, making repeated use of Lemma 6.1.8, we are able to show (Theorem 9.3.4) that B is of a particular useful form. The upshot is that both Theorem 9.4.2 in Case A and Theorem 9.3.4 in Case B enable us to prove that $(x^3)^\alpha = (x^\alpha)^3$ for all $x \in K$, which by Lemma 9.4.5 is precisely the criterion for lifting α to an isomorphism of $\langle K \rangle$ onto $\langle K' \rangle$. Our main result, Theorem 9.4.3, will thereby be proved.

We begin by showing that without loss of generality R and R' may be assumed to be centrally closed prime rings with C and C' algebraically closed fields. Indeed, since $\dim_C(RC) > 16$ we know from Theorem 9.1.13(e) that K is a prime Lie ring and from Theorem 9.2.4 that $C = C(K)$, where $C(K)$ is the Lie extended centroid of K. From the Lie isomorphism α we see that K' is also a prime Lie ring, in which case it follows that $C' = C(K')$. The Lie isomorphism α then induces an isomorphism

$c \mapsto \bar{c}$ of C onto C' according to the rule $[f, U] \mapsto [g, U^\alpha]$ where $g(u^\alpha) = f(u)^\alpha$. We claim that α may be extended to a Lie isomorphism $\phi : KC \to K'C'$ given by $\sum x_i c_i \mapsto \sum x_i^\alpha \bar{c}_i$, $x_i \in K$, $c_i \in C$. Indeed, the main point is to show that ϕ is well-defined. Suppose $\sum x_i c_i = 0$ and choose a Lie ideal $U \neq 0$ of K such that $Uc_i \subseteq K$ for all i. Then for all $u \in U$ we have

$$0 = \sum [x_i c_i, u] = \sum [x_i, c_i u] \tag{9.36}$$

Applying α to (9.36) we obtain

$$0 = \sum [x_i^\alpha, (c_i u)^\alpha] \tag{9.37}$$

But

$$(c_i u)^\alpha = f_i(u)^\alpha = g_i(u^\alpha) = \bar{c}_i u^\alpha$$

(where $c_i = [f_i, U]$, $\bar{c}_i = [g_i, U^\alpha]$) and so (9.37) becomes

$$0 = \sum [x_i^\alpha, \bar{c}_i u^\alpha] = \sum [x_i^\alpha \bar{c}_i, u^\alpha]$$

for all $u \in U$. Therefore $\sum x_i^\alpha \bar{c}_i = 0$ and ϕ is well-defined. Therefore without loss of generality we may assume that R and R' are already centrally closed. Now let F be an algebraic closure of C and let F' be an algebraic closure of C' such that the isomorphism $c \mapsto \bar{c}$ is extended to an isomorphism $\lambda \mapsto \bar{\lambda}$ of F onto F'. We then form $\widetilde{R} = R \otimes_C F$, $\widetilde{R}' = R' \otimes_{C'} F'$, and extend α to a Lie isomorphism $\phi : K \otimes_C F \to K' \otimes_{C'} F'$ via $x \otimes \lambda \mapsto x^\alpha \bar{\lambda}$, $x \in K$, $\lambda \in F$. This mapping is well-defined (the crucial observation being that $(xc)^\alpha \otimes \bar{\lambda} = x^\alpha \bar{c} \otimes \bar{\lambda} = x^\alpha \otimes \bar{c}\,\bar{\lambda} = x^\alpha \otimes \overline{(c\lambda)}$, $x \in K$, $\lambda \in C$). We leave it for the reader to verify the straightforward details that ϕ is a Lie isomorphism. Clearly we have the condition that $\dim_F(\widetilde{R}) \neq 1, 4, 9, 16, 25, 64$. Therefore we may assume to begin with that $R = \widetilde{R}$ and $R' = \widetilde{R}'$ are closed prime rings with algebraically closed extended centroids.

We next present a criterion for extending α to an associative isomorphism of $\langle K \rangle$ to $\langle K' \rangle$.

Lemma 9.4.5 *α can be extended to an isomorphism $\beta : \langle K\rangle \to \langle K'\rangle$ if and only if $(x^3)^\alpha = (x^\alpha)^3$ for all $x \in K$.*

Proof. The "only if" part being obvious, we assume

$$(x^3)^\alpha = (x^\alpha)^3 \tag{9.38}$$

for all $x \in K$. By Lemma 9.1.5 $\langle K\rangle = K \oplus K \circ K$. Replacement of x by $x \pm y$ in (9.38) results in

$$2(xy^2 + xyx + y^2x)^\alpha = 2x^\alpha(y^\alpha)^2 + 2y^\alpha x^\alpha y^\alpha + 2(y^\alpha)^2x^\alpha \tag{9.39}$$

for all $x, y \in K$. Also we have

$$\begin{aligned}(xy^2 - 2xyx + y^2x)^\alpha &= [[x, y], y]^\alpha = [[x^\alpha, y^\alpha], y^\alpha] \\ &= x^\alpha(y^\alpha)^2 - 2y^\alpha x^\alpha y^\alpha + (y^\alpha)^2x^\alpha\end{aligned} \tag{9.40}$$

Adding (9.39) and (9.40), we see that

$$(xy^2 + y^2x)^\alpha = x^\alpha(y^\alpha)^2 + (y^\alpha)^2x^\alpha \tag{9.41}$$

for all $x, y \in K$. We now define a mapping $\beta : \langle K\rangle \to \langle K'\rangle$ according to

$$x \oplus \sum y_i^2 \mapsto x^\alpha \oplus \sum(y_i^\alpha)^2, \quad x_i, y_i \in K.$$

To show that β is well-defined it suffices to show that if $\sum y_i^2 = 0$, then $\sum(y_i^\alpha)^2 = 0$. Indeed, for $x \in K$ we have $\sum y_i^2x + \sum xy_i^2 = 0$ whence by (9.41) we see that $\sum(y_i^\alpha)^2x^\alpha + x^\alpha\sum(y_i^\alpha)^2 = 0$. Clearly $s = \sum(y_i^\alpha)^2$ is a symmetric element of $\langle K'\rangle$ which anticommutes with all skew elements. Hence s commutes with all elements of the form $ab+ba$, $a, b \in K'$ and so with all symmetric elements of $\langle K'\rangle$. Since $\dim_{C'}(R') > 16$, by Theorem 9.1.13**(c)** $\langle K'\rangle$ contains a nonzero $*$-ideal I of R' and so s commutes with all symmetric elements $S(I)$ of I. One can easily shows that $\dim_{C'}(C'I) > 16$

and hence $\langle S(I)\rangle$ contains a nonzero ideal J of the ring I by Lemma 9.1.14. From Andrunakievich's Lemma we conclude that J contains a nonzero ideal J' of R' (see [276]). Since s commutes with J' and R' is a prime ring, we see that s is a central element of R'. Recalling that $sz = -zs$ for all $z \in K'$ we infer that $s = 0$ and thus β is a well-defined mapping of $\langle K\rangle$ onto $\langle K'\rangle$.

From the identity $xy = \frac{1}{2}\{(x+y)^2 - x^2 - y^2 + [x,y]\}$ and from the definition of β we see that for $x, y \in K$

$$\begin{aligned}(xy)^\beta &= \frac{1}{2}\{[(x+y)^2]^\beta - (x^2)^\beta - (y^2)^\beta + [x,y]^\beta\}\\ &= \frac{1}{2}\{(x^\alpha + y^\alpha)^2 - (x^\alpha)^2 - (y^\alpha)^2 + [x^\alpha, y^\alpha]\}\\ &= x^\alpha y^\alpha = x^\beta y^\beta \qquad (9.42)\end{aligned}$$

Next from the identity $x^2y = \frac{1}{2}\{x \circ [x,y] + x^2 \circ y\}$ we obtain

$$\begin{aligned}(x^2y)^\beta &= \frac{1}{2}\{(x\circ[x,y])^\beta + (x^2\circ y)^\alpha\}\\ &= \frac{1}{2}\{x^\alpha \circ [x^\alpha, y^\alpha] + (x^\alpha)^2 \circ y^\alpha\}\\ &= (x^\alpha)^2 y^\alpha = (x^2)^\beta y^\beta \qquad (9.43)\end{aligned}$$

making use of (9.41). Together (9.42) and (9.43) imply

$$(ux)^\beta = u^\beta x^\beta, \quad u \in \langle K\rangle,\ x \in K \qquad (9.44)$$

and, since $\langle K\rangle$ is generated by K, it follows from (9.44) that β is a homomorphism of $\langle K\rangle$ onto $\langle K'\rangle$. By symmetry the Lie isomorphism $x^\alpha \mapsto x$ of K' onto K can be extended to a homomorphism $\gamma : \langle K'\rangle \to \langle K\rangle$. Since $\beta\gamma$ is the identity on K and $\gamma\beta$ is the identity on K' it is clear that β is an isomorphism.

At this point we divide our analysis of α into two separate cases:

Case A: R is *GPI*.

Case B: R is not GPI.

Case A. By Theorem 6.1.6 R has nonzero socle H. Since $\dim_C(R) > 36$ we know from the $*$-Litoff Theorem that H contains a symmetric idempotent e of rank $n \geq 6$. Then $eRe \cong M_n(C)$ and by Corollary 4.6.13 the involution $*$ on eRe is either transpose or symplectic. In either of these cases it is well-known that eRe contains orthogonal symmetric idempotents e_1 and e_2 each of rank 2. It is then easy to check that for $i = 1, 2$ e_i lies in the subring generated by $[K, K] \cap e_iRe_i$. Finally α clearly induces a Lie isomorphism α_0 from $[K, K]$ onto $[K', K']$, and so the conditions of Theorem 9.4.2 have now been met. We may therefore conclude that α_0 can be extended to an associative isomorphism $\sigma : T \to T'$, where $T = \langle [K, K] \rangle$ and $T' = \langle [K', K'] \rangle$. It is easily seen that $(K \cap T)^\sigma = K' \cap T'$. Indeed, this follows from writing $x \in K \cap T$ as

$$x = \sum (u_1 u_2 \dots u_n + (-1)^{n+1} u_n \dots u_1), \quad u_i \in [K, K],$$

and then applying the isomorphism σ. Similarly $(S \cap T)^\sigma = S' \cap T'$, where S and S' are respectively the symmetric elements of R and R'. We also claim that α agrees with σ on $K \cap T$. Indeed, for $x \in K \cap T$, $y \in [K, K]$ we have

$$[x^\alpha, y^\alpha] = [x, y]^\alpha = [x, y]^\sigma = [x^\sigma, y^\sigma] = [x^\sigma, y^\alpha],$$

whence $x^\alpha - x^\sigma$ commutes with $[K', K']$ and so $x^\alpha - x^\sigma$ is central by Theorem 9.1.13(**c**). But we have already seen that x^σ (as well x^α) must be skew, and so $x^\alpha - x^\sigma = 0$ which proves our claim.

By Theorem 9.1.13(**c**) $H \subseteq T$. We note that H itself is a simple ring. If $I \neq 0$ is an ideal of T, then $I \cap H \neq 0$ is an ideal of H and so $I \cap H = H$, i.e., $I \supseteq H$. It follows that H is also the socle of T. It is easy to show via σ that R' must be GPI with socle H^σ.

We now fix $t \in K$. We claim first of all that

$$[u, t]^\sigma = [u^\sigma, t^\alpha], \quad u \in H \tag{9.45}$$

Indeed, since $\langle H \cap K \rangle = H$ by Lemma 9.1.4 and the simplicity of H, we may assume without loss of generality that $u = x_1 x_2 \ldots x_n$, $x_i \in H \cap K$. For $n = 1$

$$[x_1, t]^\sigma = [x_1, t]^\alpha = [x_1^\alpha, t^\alpha] = [x_1^\sigma, t^\alpha].$$

Inductively we have

$$\begin{aligned} [x_1 x_2 \ldots x_n, t]^\sigma &= \{x_1[x_2 \ldots x_n, t] + [x_1, t]x_2 \ldots x_n\}^\sigma \\ &= x_1^\sigma [x_2 \ldots x_n, t]^\sigma + [x_1, t]^\sigma (x_2 \ldots x_n)^\sigma \\ &= x_1^\sigma [(x_2 \ldots x_n)^\sigma, t^\alpha] + [x_1^\sigma, t^\alpha](x_2 \ldots x_n)^\sigma \\ &= [x_1^\sigma (x_2 \ldots x_n)^\sigma, t^\alpha] = [(x_1 x_2 \ldots x_n)^\sigma, t^\alpha] \end{aligned}$$

and so our claim is established.

From $[u \circ t, u] = [t, u] \circ u$ we see, making use of (9.45), that

$$[(u \circ t)^\sigma, u^\sigma] = [t^\alpha, u^\sigma] \circ u^\sigma = [u^\sigma \circ t^\alpha, u^\sigma]$$

for all $u \in H$. In other words $\psi_t : u^\sigma \mapsto (u \circ t)^\sigma - u^\sigma \circ t^\alpha$ is an additive commuting function on the ring H^σ. By Corollary 9.3.3 there exist $\lambda \in C'$ and $\mu : H^\sigma \to C'$ such that

$$(u \circ t)^\sigma - u^\sigma \circ t^\alpha = \lambda u^\sigma - \mu(u^\sigma), \quad u \in H \tag{9.46}$$

Choosing $u \in H \cap K$ we see that $\lambda = 0$ by comparing the skew and symmetric parts of (9.46). Next, choosing $u \in S \cap H$, we see from (9.46) that $\mu(u^\sigma) = 0$, that is

$$(u \circ t)^\sigma = u^\sigma \circ t^\alpha, \quad u \in S \cap H \tag{9.47}$$

Together (9.45) and (9.46) imply that

$$(ut)^\sigma = u^\sigma t^\alpha, \quad u \in S \cap H$$

whence

$$(u_1 u_2 \ldots u_n t)^\sigma = u_1^\sigma u_2^\sigma \ldots u_n^\sigma t^\alpha, \quad u_i \in S \cap H \tag{9.48}$$

But $\langle S \cap H \rangle = H$ by Lemma 9.1.14 and so (9.48) implies

$$(ut)^\sigma = u^\sigma t^\alpha, \quad u \in H,\ t \in K.$$

Similarly $(tv)^\sigma = t^\alpha v^\sigma$, $v \in H$, $t \in K$ and so

$$\begin{aligned} u^\sigma (t^3)^\alpha v^\sigma &= (ut^3)^\sigma v^\sigma = (ut^3 v)^\sigma = \{(ut)t(tv)\}^\sigma \\ &= \{(ut)t\}^\sigma (tv)^\sigma = (ut)^\sigma t^\alpha t^\alpha v^\sigma = u^\sigma (t^\alpha)^3 v^\sigma \end{aligned}$$

for all $u, v \in H$, $t \in K$. Therefore $H^\sigma[(t^3)^\alpha - (t^\alpha)^3]H^\sigma = 0$ whence $(t^3)^\alpha = (t^\alpha)^3$ for all $t \in K$. Lemma 9.4.5 is thereby applicable and so we have succeeded in showing in Case A that α can be extended to an isomorphism of $\langle K \rangle$ onto $\langle K' \rangle$.

Case B. we begin by pointing out that necessarily R' is not GPI. Indeed, since R is not GPI, it follows that $\dim_C(K) = \infty$, whence $\dim_{C'}(K') = \infty$. If R' is GPI we have already seen in our discussion of **Case A** (with α^{-1} now playing the role of α) that α^{-1} may be lifted to an isomorphism σ' of $\langle K' \rangle$ onto $\langle K \rangle$. Using σ' we easily reach the contradiction that R must be GPI.

We define a C'-trilinear symmetric mapping $B : (K')^3 \to K'$ as follows:

$$B(x^\alpha, y^\alpha, z^\alpha) = \frac{1}{6}(xyz + xzy + yxz + yzx + zxy + zyx)^\alpha$$

for all $x, y, z \in K$. Its trace $B(x^\alpha, x^\alpha, x^\alpha)$ is obviously commuting since $B(x^\alpha, x^\alpha, x^\alpha) = (x^3)^\alpha$ and $[(x^3)^\alpha, x^\alpha] = [x^3, x]^\alpha = 0$ for all $x \in K$. Thus by Theorem 9.3.4 there exist $\lambda \in C'$ and a C'-bilinear mapping $\mu : K' \times K' \to C'$ such that

$$\begin{aligned} &(xyz + xzy + yxz + yzx + zxy + zyx)^\alpha \\ &\quad = \lambda(x^\alpha y^\alpha z^\alpha + x^\alpha z^\alpha y^\alpha + y^\alpha x^\alpha z^\alpha \\ &\quad + y^\alpha z^\alpha x^\alpha + z^\alpha x^\alpha y^\alpha + z^\alpha y^\alpha x^\alpha) \\ &\quad + \mu(y,z)x^\alpha + \mu(x,z)y^\alpha + \mu(x,y)z^\alpha \qquad (9.49) \end{aligned}$$

for all $x, y, z \in K$, where for notational ease we are simply writing $\mu(x, y)$ for $\mu(x^\alpha, y^\alpha)$. Our aim, of course, is to show that

$\lambda = 1$ and that $\mu = 0$, whence $(x^3)^\alpha = (x^\alpha)^3$ and Lemma 9.4.5 may accordingly be invoked to obtain the desired conclusion that α may be extended to an isomorphism of $\langle K \rangle$ onto $\langle K' \rangle$.

We now proceed to draw some consequences from (9.49). First setting $x = z$ in (9.49) and dividing by 2, we obtain

$$\begin{aligned}(x^2y + xyx + yx^2)^\alpha &= \lambda\{(x^\alpha)^2y^\alpha + x^\alpha y^\alpha x^\alpha + y^\alpha(x^\alpha)^2\} \\ &\quad +\mu(x,y)x^\alpha + \frac{1}{2}\mu(x,x)y^\alpha \qquad (9.50)\end{aligned}$$

Now, setting $x = y$ in (9.50), we have

$$(x^3)^\alpha = \lambda(x^\alpha)^3 + \frac{1}{2}\mu(x,x)x^\alpha \qquad (9.51)$$

From $3xyx = x^2y + xyx + yx^2 - [[y,x],x]$ we conclude using (9.50) that

$$\begin{aligned}3(xyx)^\alpha &= \lambda\{(x^\alpha)^2y^\alpha + x^\alpha y^\alpha x^\alpha + y^\alpha(x^\alpha)^2\} + \mu(x,y)x^\alpha \\ &\quad +\frac{1}{2}\mu(x,x)y^\alpha - \{(x^\alpha)^2y^\alpha - 2x^\alpha y^\alpha x^\alpha + y^\alpha(x^\alpha)^2\} \\ &= (\lambda+2)x^\alpha y^\alpha x^\alpha + (\lambda-1)\{(x^\alpha)^2y^\alpha + y^\alpha(x^\alpha)^2\} \\ &\quad +\mu(x,y)x^\alpha + \frac{1}{2}\mu(x,x)y^\alpha\end{aligned}$$

whence

$$\begin{aligned}(xyx)^\alpha &= \frac{\lambda+2}{3}x^\alpha y^\alpha x^\alpha + \frac{\lambda-1}{3}\{(x^\alpha)^2y^\alpha + y^\alpha(x^\alpha)^2\} \\ &\quad +\frac{1}{3}\mu(x,y)x^\alpha + \frac{1}{6}\mu(x,x)y^\alpha \qquad (9.52)\end{aligned}$$

Lemma 9.4.6 $\lambda = 1$, *i.e.*,

$$(xyx)^\alpha = x^\alpha y^\alpha x^\alpha + \frac{1}{3}\mu(x,y)x^\alpha + \frac{1}{6}\mu(x,x)y^\alpha.$$

Proof. Choose $x^\alpha \in K'$ such that x^α is not algebraic of degree ≤ 6 (such x^α exists since otherwise K' would be PI). In the free product $R'_{C'}{<}Y{>}$ consider the C'-independent subset $\{M_i(x^\alpha, Y) \mid i = 1, 2, \ldots, n\}$ of all monomials of the form $(x^\alpha)^{j_0} Y^{i_1} (x^\alpha)^{j_1} \ldots Y^{i_k} (x^\alpha)^{j_k}$ where $j_0 + j_1 + \ldots + j_k \leq 6$ and $i_1 + i_2 + \ldots + i_k \leq 6$. By Lemma 6.1.8 there exists $y^\alpha \in K'$ such that $\{M_i(x^\alpha, y^\alpha)\}$ is a C'-independent subset of R'. We compute $(x^3yx^3)^\alpha$ in two different ways and compare the results, being only interested in the coefficients of $(x^\alpha)^6 y^\alpha$ and $(x^\alpha)^5 y^\alpha x^\alpha$. On the one hand

$$\begin{aligned}(x^3yx^3)^\alpha &= \frac{\lambda+2}{3} u y^\alpha u + \frac{\lambda-1}{3}\{u^2 y^\alpha + y^\alpha u^2\} \\ &\quad + \frac{1}{3}\mu(x^3, y)u + \frac{1}{6}\mu(x^3, x^3) y^\alpha \qquad (9.53)\end{aligned}$$

where $u = \lambda(x^\alpha)^3 + \frac{1}{2}\mu(x,x)x^\alpha$ (see (9.51) and (9.52)). Using

$$u^2 = \lambda^2 (x^\alpha)^6 + \lambda\mu(x,x)(x^\alpha)^4 + \frac{1}{4}\mu(x,x)^2 (x^\alpha)^2$$

we may write (9.53) as

$$(x^3yx^3)^\alpha = \frac{\lambda-1}{3}\lambda^2 (x^\alpha)^6 y^\alpha + 0 \cdot (x^\alpha)^5 y^\alpha x^\alpha + \ldots \qquad (9.54)$$

On the other hand

$$\begin{aligned}(x^3yx^3)^\alpha &= \{x(x^2yx^2)x\}^\alpha \\ &= \frac{\lambda+2}{3} x^\alpha v x^\alpha + \frac{\lambda-1}{3}(x^\alpha)^2 v + \frac{\lambda-1}{3} v (x^\alpha)^2 \\ &\quad + \frac{1}{3}\mu(x, x^2yx^2)x^\alpha + \frac{1}{6}\mu(x,x)v \qquad (9.55)\end{aligned}$$

where

$$\begin{aligned}v &= (x^2yx^2)^\alpha = \{x(xyx)x\}^\alpha \\ &= \frac{\lambda+2}{3} x^\alpha w x^\alpha + \frac{\lambda-1}{3}(x^\alpha)^2 w + \frac{\lambda-1}{3} w (x^\alpha)^2 \\ &\quad + \frac{1}{3}\mu(x, xyx)x^\alpha + \frac{1}{6}\mu(x,x)w\end{aligned}$$

where in turn

$$\begin{aligned} w = (xyx)^\alpha &= \frac{\lambda+2}{3}x^\alpha y^\alpha x^\alpha + \frac{\lambda-1}{3}(x^\alpha)^2 y^\alpha + \frac{\lambda-1}{3}y^\alpha (x^\alpha)^2 \\ &\quad + \frac{1}{3}\mu(x,y)x^\alpha + \frac{1}{6}\mu(x,x)y^\alpha. \end{aligned}$$

Therefore

$$\begin{aligned} (x^3yx^3)^\alpha &= \left(\frac{\lambda-1}{3}\right)^3 (x^\alpha)^6 y^\alpha \\ &\quad + \left[\frac{\lambda+2}{3}\left(\frac{\lambda-1}{3}\right)^2 + \frac{\lambda-1}{3}\frac{\lambda+2}{3}\frac{\lambda-1}{3} \right. \\ &\quad \left. + \left(\frac{\lambda-1}{3}\right)^2 \frac{\lambda+2}{3}\right] (x^\alpha)^5 y^\alpha x^\alpha + \ldots \\ &= \left(\frac{\lambda-1}{3}\right)^3 + \frac{(\lambda+2)(\lambda-1)^2}{9}(x^\alpha)^5 y^\alpha x^\alpha \\ &\quad + \ldots \end{aligned} \tag{9.56}$$

Equating the coefficients of $(x^\alpha)^6 y^\alpha$ and $(x^\alpha)^5 y^\alpha x^\alpha$ in (9.54) and (9.56) we have

$$\left(\frac{\lambda-1}{3}\right)^3 = \left(\frac{\lambda-1}{3}\right)\lambda^2 \tag{9.57}$$

$$\frac{(\lambda+2)(\lambda-1)^2}{9} = 0 \tag{9.58}$$

From (9.57) we find that $\lambda = 1$ or $\lambda^2 = \left(\frac{\lambda-1}{3}\right)^2$, whence $\lambda = 1, -\frac{1}{2}$ or $\frac{1}{4}$. From (9.58) we have $\lambda = 1$ or $\lambda = 2$. It follows that $\lambda = 1$ and the lemma is proved.

Lemma 9.4.7 $\mu = 0$.

Proof. Let $x^\alpha \neq 0$ be arbitrary but fixed in K'. In the free product $R'_{C'}\langle Y\rangle$ we define the C'-independent set $\{M_i(x^\alpha, Y) \mid i = 1, 2, \ldots, n\}$ to be the set of all monomials of the form $(x^\alpha)^{j_0} Y^{i_1} (x^\alpha)^{j_1} \ldots Y^{i_k} (x^\alpha)^{j_k}$ where $j_0 + j_1 + \ldots + j_k \leq 4$, $i_1 + i_2 + \ldots + i_k \leq 3$ and

$$\begin{aligned} j_q &\leq 3 \quad \text{if } x \text{ is not algebraic of degree} \leq 3 && (9.59)\\ j_q &\leq 2 \quad \text{if } x \text{ is algebraic of degree } 3 && (9.60)\\ j_q &\leq 1 \quad \text{if } x \text{ is algebraic of degree } 2 && (9.61)\end{aligned}$$

for all $q = 0, 1, \ldots, k$. In case of (9.60) we can replace $(x^\alpha)^3$ by βx^α, $\beta \in C'$, and in case of (9.61) we can replace $(x^\alpha)^2$ by $\gamma \in C'$ and hence $(x^\alpha)^3$ by γx^α. By Lemma 6.1.8 there exists $y^\alpha \in K'$ such that $\{M_i(x^\alpha, y^\alpha)\}$ is a C'-independent subset of R'. We compute $(xyxyxyx)^\alpha$ in two ways and compare the results, being only interested in coefficients of $(y^\alpha)^2 x^\alpha y^\alpha x^\alpha$.

On the one hand, making use of Lemma 9.4.6, we have

$$\begin{aligned}
&[(xyx)y(xyx)]^\alpha\\
&= (xyx)^\alpha y^\alpha (xyx)^\alpha + \frac{1}{3}\mu(y, xyx)(xyx)^\alpha + \frac{1}{6}\mu(xyx, xyx)y^\alpha\\
&= \{x^\alpha y^\alpha x^\alpha + \frac{1}{3}\mu(x,y)x^\alpha + \frac{1}{6}\mu(x,x)y^\alpha\}y^\alpha\\
&\cdot\{x^\alpha y^\alpha x^\alpha + \frac{1}{3}\mu(x,y)x^\alpha + \frac{1}{6}\mu(x,x)y^\alpha\}\\
&+\frac{1}{3}\mu(y, xyx)\{x^\alpha y^\alpha x^\alpha + \frac{1}{3}\mu(x,y)x^\alpha + \frac{1}{6}\mu(x,x)y^\alpha\}\\
&+\frac{1}{6}\mu(xyx, xyx)y^\alpha\\
&= x^\alpha y^\alpha x^\alpha y^\alpha x^\alpha y^\alpha x^\alpha + \frac{1}{6}\mu(x,x)(y^\alpha)^2 x^\alpha y^\alpha x^\alpha + \ldots \qquad (9.62)
\end{aligned}$$

On the other hand, again using Lemma 9.4.6, we have

$$[x(yxyxy)x]^\alpha$$

$$\begin{aligned}
&= x^\alpha(yxyxy)^\alpha x^\alpha + \frac{1}{3}\mu(x, yxyxy)x^\alpha + \frac{1}{6}\mu(x,x)(yxyxy)^\alpha \\
&= x^\alpha\{y^\alpha(xyx)^\alpha y^\alpha + \frac{1}{3}\mu(y, xyx)y^\alpha + \frac{1}{6}\mu(y,y)(xyx)^\alpha\}x^\alpha \\
&\quad +\frac{1}{3}\mu(x, yxyxy)x^\alpha \\
&+\frac{1}{6}\mu(x,x)\{y^\alpha(xyx)^\alpha y^\alpha + \frac{1}{3}\mu(y, xyx)y^\alpha + \frac{1}{6}\mu(y,y)(xyx)^\alpha\} \\
&= x^\alpha y^\alpha\{x^\alpha y^\alpha x^\alpha + \frac{1}{3}\mu(x,y)x^\alpha + \frac{1}{6}\mu(x,x)y^\alpha\}y^\alpha x^\alpha \\
&+\frac{1}{3}\mu(y, xyx)x^\alpha y^\alpha x^\alpha \\
&+\frac{1}{6}\mu(y,y)x^\alpha\{x^\alpha y^\alpha x^\alpha + \frac{1}{3}\mu(x,y)x^\alpha + \frac{1}{6}\mu(x,x)y^\alpha\}x^\alpha \\
&+\frac{1}{3}\mu(x, yxyxy)x^\alpha \\
&+\frac{1}{6}\mu(x,x)y^\alpha\{x^\alpha y^\alpha x^\alpha + \frac{1}{3}\mu(x,y)x^\alpha + \frac{1}{6}\mu(x,x)y^\alpha\}y^\alpha \\
&+\frac{1}{18}\mu(x,x)\mu(y, xyx)y^\alpha \\
&+\frac{1}{36}\mu(x,x)\mu(y,y)\{x^\alpha y^\alpha x^\alpha + \frac{1}{3}\mu(x,y)x^\alpha + \frac{1}{6}\mu(x,x)y^\alpha\} \quad (9.63)
\end{aligned}$$

It is understood that (9.63) will be further rewritten by replacing $(x^\alpha)^3$ by βx in case (9.60) holds and replacing $(x^\alpha)^2$ by γ and $(x^\alpha)^3$ by γx^α in case (9.61) holds. Now, comparing the coefficients of $(y^\alpha)^2 x^\alpha y^\alpha x^\alpha$ in (9.62) and (9.63) we see that $\mu(x,x) = \mu(x^\alpha, x^\alpha) = 0$ for all $x^\alpha \in K'$. Linearizing we have $\mu(x^\alpha, y^\alpha) = 0$ for all $x^\alpha, y^\alpha \in K'$ and the proof of Lemma 9.4.7 is complete.

Together Lemma 9.4.6 and Lemma 9.4.7 imply that $(x^3)^\alpha = (x^\alpha)^3$ for all $x \in K$ and so by Lemma 9.4.5 we have succeeded in **Case B** that α can be extended uniquely to an isomorphism of $\langle K\rangle$ onto $\langle K'\rangle$. Our analysis of **Case A** and **Case B** combine to immediately give us the proof of our main result. Theorem 9.4.3, a complete statement of which is given near the beginning of this section.

As a closing note we make two remarks. The analogue of Theorem 9.4.3 for Lie derivations of K has been proved by Swain [269]. The condition in Theorem 9.4.1 that R not satisfy St_4 has been removed by Blau [55].

List of Symbols

$End(R)$	Endomorphisms of R	2
$Der(R)$	Derivations of R	2
$ad(a)$	Inner derivation	2
$Aut(R)$	Automorphisms of R	3
$Antiaut(R)$	Antiautomorphisms of R	3
$G(R)$	$Aut(R) \cup Antiaut(R)$,	3
$Z(R)$	Center of R	3
$R \propto G$	Skew group ring	4
$V \otimes_K W$	Tensor product	8
$K\{V\}$	Tensor algebra	9
R^o	Opposite ring	10
$S<X>$	Free semigroup with 1	11
$K<X>$	Free algebra	11
$R_{A\sigma B}$	Reduction	15
$\Phi<X>_{irr}$	Irreducible elements	15
Λ	Reduction system	15
$\Phi<X>_{red}$	Elements with unique normal form	16
$I(\Lambda)$		16
$\mathcal{Z}$	Integers	21
Q	Rationals	21
St_n	Standard polynomial	21
$M_n(R)$	$n \times n$ matrices	21
$A_1 \coprod_K A_2$	Coproduct	26
$\mathcal{N}$	Natural numbers	35
Ω_F		35

$W(\alpha)$		35
$\mathcal{T}_\Omega$		36
$Map(X;R)$		36
$\wedge$	Conjunction	38
$\vee$	Disjunction	38
$\neg$	Negation	38
$\Rightarrow$	Implication	38
$\forall$	For every	38
$\exists$	There exists	38
$\mathcal{P}_\Delta$	Formal predicate symbols	38
$Compl(\phi)$	Complexity	38
$R \models \phi$		41
$\mathcal{T}_\infty$		45
$\mathcal{T}_{i_0}$	Principal ultrafilter	45
$\prod_{i\in I} R_i/\mathcal{T}$	Ultraproduct	47
$l_R(S)$	Left annihilator	51
$r_R(S)$	Right annihilator	51
$\mathcal{D}(R)$	Dense right ideals	51
$(S:J)_R$		51
$f^{-1}(J)$		52
Q_{mr}	Maximal right ring of quotients	56
$Z_r(R)$	Right singular ideal	60
$Q_r(R)$	Two-sided right ring of quotients	64
$Q_s(R)$	Symmetric ring of quotients	66
C	Extended centroid	68
RC	Central closure	68
$R_{(l)}$	Left multiplications	69
$R_{(r)}$	Right multiplications	69
$E(V)$		74
$D_i(R)$	X-inner derivations	88
$D(R)$	$Der(R)C + D_i$	89
$G_i(R)$	X-inner automorphisms	91
$N_{I,J}$		91
N_I		91

$x \cdot \beta$		91
β^{ϵ}		91
$inn(t)$	Inner automorphism	91
M_{σ}	Conjugation module	92
$B(C)$	Central idempotents	99
$\sum^{\perp}_{u\in U} t_u u$		100
M_{μ}		105
$O(T)$	Orthogonal completion	106
$Spec(B)$	Spectrum	111
RM		111
R_M	Pierce stalk	112
ϕ_M	Canonical projection	112
$H(\Phi;\vec{a})$		114
$E(\Phi(\vec{a}))$		114
$N(R)$	Commuting ring	129
$\langle\ ,\ \rangle$	Bilinear form	139
a^*	Adjoint	139
$\mathcal{L}_W(V)$		140
$\mathcal{F}_W(V)$		140
$Soc(R)$	Socle	142
$S^{\perp}$		149
$\pi(x)$	Generalized pivotal monomial	151
$\mathcal{F}_V$		159
$\mathcal{L}_V$		159
$U(K)$	Universal enveloping algebra	175
$(K;F;\Lambda)$	Differential Lie algebra	187
$\mathcal{B}$	C-basis of D	208
$\mathcal{B}_0$	Well-ordered C-basis of D mod D_i	209
$\mathcal{B}_i$	Well-ordered C-basis of D_i	209
$\mathcal{W}$	PBW-basis of U	209
$\mathcal{W}_0$		209
$\mathcal{W}_i$	PBW-basis of U_i	209
$Q_C{<}X{>}$		212
GPI	Generalized polynomial identity	212

$\deg_x$	x-degree	214
$\deg$	degree	214
ht_x	x-height	214
ht	height	214
Φ_P		232
$\mathcal{G}(H;R)$	$\mathcal{T}$-ideal of GPI's	259
$\mathcal{T}(H;L)$	$\mathcal{T}$-ideal generated by L	259
$ST_2(e;X)$		259
$L_q(e;X)$		259
$ST_{2n}(w,X)$		278
G_0	Representatives of G mod G_i	298
$Aut_0(R)$	$G_0 \cap Aut(R)$,	298
$Antiaut_0(R)$	$G_0 \cap Antiaut(R)$,	298
T	$U \propto G$,	301
$C\{V \otimes T\}$	Algebra of variables	301
$\mathcal{S}(R)$	Setting of R	301
T_1	$\mathcal{W}G$,	303
$\mathcal{S}_0(C)$	Setting of C	304
$\mathcal{S}_1(R)$	Extended setting	304
I_0	Trivial T-identities	305
$\mathcal{B}^h$		306
$\mathcal{B}_0^h$		306
$\mathcal{B}_i^h$		306
$\mathcal{W}^h$		306
$\mathcal{W}_0^h$		306
$\mathcal{W}_i^h$		306
T_0	$\mathcal{W}_0G_0$,	307
$\mathcal{E}$	Reduced elements of $\mathcal{S}$	307
G^*	$Aut(R)$,	309
T^*	$U \propto G^*$,	309
G_0^*	$G_0 \cap G^*$,	309
T_1^*	$\mathcal{W}G^*$,	309
T_0^*	$\mathcal{W}_0G_0^*$,	309
$\mathcal{S}^*$		310

$\mathcal{E}^*$		310
I_0^*		310
$sup(\phi)$	Support	317
$\Delta_{\phi,g}$	Leading g-term	317
G_f	Frobenius automorphisms (fields)	332
G_{0f}	Representatives of G mod G_f (fields)	333
$I_2(C)$	F-trivial T-identities (fields)	334
N		334
$\mathcal{N}_p$		334
$V_{\alpha,s}$		335
V_s		335
G_f	Frobenius elements (general)	345
G_{0f}	Representatives of G mod G_f (general)	345
F-deg	Frobenius degree	347
$\mathcal{S}_m$	Maximal setting	360
$\mathcal{S}_m^*$	$*$-Maximal setting	361
I_0'	Trivial T'-identities	362
$\mathcal{E}_m$	Reduced elements of $\mathcal{S}_m$	362
S-deg	(derivations)	365
S-deg	(automorphisms)	371
$\widehat{D}$		387
$\hat{U}$	Universal enveloping algebra (semiprime)	388
$u_1(g)$		400
$u_2(g)$		400
G_f	Frobenius elements (semiprime)	402
$\widehat{G}(R)$		403
$e(g)$		405
α_M		408
$e_{0,\alpha}$		409
$e_{1,\alpha}$		409
$e_{2,\alpha}$		409
$e_{3,\alpha}$		409
$U(v)$		410
$\widehat{T}$	$\hat{U} \propto \widehat{G}$,	417

$\widehat{\mathcal{S}}_m$	Maximal setting (semiprime)	418
$\widehat{I}_0$		418
$M(f)$		419
G^*	(semiprime)	421
$\widehat{T}^*$		422
$N_I(f)$		423
$[x, y]$	Lie product	438
$x \circ y$	Jordan product	438
$W^{(i)}$		440
$X \equiv 0$		440
$\langle W \rangle$	Subring generated by W	440
$L(K)$		441
$\widetilde{R}$	$RC \otimes_C F$	445

Bibliography

[1] S. A. Amitsur, Derivations in simple rings. *London Math. Soc.* **7** (1957), 87–112.

[2] S. A. Amitsur, Rings with a pivotal monomial. *Proc. Amer. Math. Soc.* **9** (1958), 635–642.

[3] S. A. Amitsur, Generalized polynomial identities and pivotal monomials. *Trans. Amer. Math. Soc.* **114** (1965), 210–226.

[4] S. A. Amitsur, Nil semi-groups of rings with a polynomial identity. *Nagoya Math. J.* **27** (1966), 103–111.

[5] S. A. Amitsur, Rational identities and applications to algebra and geometry. *J. Algebra* **3** (1966), 304–359.

[6] S. A. Amitsur, Rings with involution. *Israel J. Math.* **6** (1968), 99–106.

[7] S. A. Amitsur, Identities in rings with involution. *Israel J. Math.* **7** (1969), 63–68.

[8] S. A. Amitsur, On rings of quotients. *Symposia Mathematica* **8** (1972), 149–164.

[9] S. A. Amitsur and Levitzki, Minimal identities for algebras. *Proc. Amer. Math. Soc.* **1** (1950), 449–463.

[10] P. N. Ánh and L. Márki, On Martindale's theorem. *Rocky Mountain J. Math., to appear.*

[11] P. N. Ánh and L. Márki, Orders in primitive rings with non-zero socle and Posner's theorem. *Comm. Algebra, to appear.*

[12] V. I. Arnautov, K. I. Beidar, S. T. Glavatsky, and A. V. Mikhalev, Intersection property in the radical theory of topological algebras. *Contemporary Math.* **131** (1992), 205–225.

[13] R. Awtar, Lie and Jordan structure in prime rings with derivations. *Proc. Amer. Math. Soc.* **41** (1973), 67–74.

[14] R. Baer, Algebraische theorie der differentierbaren funktionenkörper, I. *Sitzungsberichte, Heidelberger Akademia* (1927), 15–32.

[15] W. E. Baxter and W. S. Martindale 3rd, Rings with involution and polynomial identities. *Canad. J. Math.* **20** (1968), 465–473.

[16] W. E. Baxter and W. S. Martindale 3rd, Central closure of semiprime nonassociative rings. *Comm. Algebra* **7** (1979), 1103–1132.

[17] W. E. Baxter and W. S. Martindale 3rd, The extended centroid of $*$-prime rings. *Comm. Algebra* **10** (1982), 847–874.

[18] W. E. Baxter and W. S. Martindale 3rd, The extended centroid in semiprime rings with involution. *Comm. Algebra* **13** (1985), 945–985.

[19] Y. A. Bahturin. *Identical Relations in Lie Algebras.* VNU Science Press, Utrecht, 1987.

[20] Yu. A. Bahturin, A. A. Mikhalev, M. V. Zaitsev, and V. M. Petrogradsky, *Infinite Dimensional Lie Superalgebras*. Walter de Gruyter Publ. Berlin – New York, 1992.

[21] K. I. Beidar, Rings with generalized identities, I. *Moscow Univ. Math. Bull.* **32** (1) (1977), 15–20.

[22] K. I. Beidar, Rings with generalized identities, II. *Moscow Univ. Math. Bull.* **32** (3) (1977), 27–33.

[23] K. I. Beidar, Semiprime rings with generalized identity. *Russian Math. Surveys* **32** (4) (1977), 249–250.

[24] K. I. Beidar, Rings with generalized identities, III. *Moscow Univ. Math. Bull.* **33** (4) (1978), 53–58.

[25] K. I. Beidar, Rings of quotients of semiprime rings. *Moscow Univ. Math. Bull.* **33** (5) (1978), 29–34.

[26] K. I. Beidar. *Rings with generalized polynomial identities*, PhD thesis, Moscow State Univ., 1978.

[27] K. I. Beidar, Rings with generalized identities, IV. *Moscow Univ. Math. Bull.* **35** (4) (1980), 1–4.

[28] K. I. Beidar, Y. Fong, U. Knauer, and A. V. Mikhalev, On semigroups with generalized identities. In *Proceedings of the Tainan-Moscow Algebra Workshop*, Walter de Gruyter, to appear.

[29] K. I. Beidar, Y. Fong, and X. K. Wang, Posner and Herstein theorems for derivations of 3-prime near-rings. *Comm. Algebra, to appear.*

[30] K. I. Beidar and P. Grzeszczuk, Actions of Lie algebras on rings without nilpotent elements. *Algebra Colloq.* **2** (2) (1995), 105–116.

[31] K. I. Beidar, W. S. Martindale 3rd, and A. V. Mikhalev, Lie isomorphisms in prime rings with involution. *J. Algebra* **169** (1994), 304–327.

[32] K. I. Beidar and A. V. Mikhalev, Homogeneous boundness almost everywhere for orthogonal complete algebraic systems. *Vestnik Kievskogo Universiteta, Ser. Mat., Mekh.* **27** (1985), 15–17 (Ukrainian).

[33] K. I. Beidar and A. V. Mikhalev, Orthogonal completeness and algebraic systems. *Russian Math. Surveys* **40** (6) (1985), 51–95.

[34] K. I. Beidar and A. V. Mikhalev, Generalized polynomial identities and rings which are sums of two subrings. *Algebra i Logika* **34** (1) (1995), 3–11 (Russian).

[35] K. I. Beidar and A. V. Mikhalev, The method of orthogonal completeness in structure theory of rings. *Journal of Math. Sciences* **73** (1) (1995), 1–44.

[36] K. I. Beidar, A. V. Mikhalev, and K. Salavova, Generalized identities and semiprime rings with involution. *Russian Math. Surveys* **35** (1) (1980), 222 (Russian).

[37] K. I. Beidar, A. V. Mikhalev, and K. Salavova, Generalized identities and semiprime rings with involution. *Math. Z.* **178** (1981), 37–62.

[38] K. I. Beidar, A. V. Mikhalev, and A. M. Slin'ko, A criterion for primeness of nondegenerate alternative and Jordan algebras. *Trans. Moscow Math. Soc.* **50** (1988), 129–137.

[39] H. E. Bell and W. S. Martindale 3rd, Centralizing mappings of semiprime rings. *Canad. Math. Bull.* **30** (1987), 92–101.

[40] H. E. Bell and W. S. Martindale 3rd, Semiderivations and commutativity in prime rings. *Canad. Math. Bull.* **31** (1988), 500–508.

[41] H. E. Bell and G. Mason, On derivations in near-rings. In G. Betsch, editor, *Near-Rings and Near-Fields*, North-Holand/American Elsevier, Amsterdam, 1987.

[42] L. P. Belluce and S. K. Jain, A remark on primitive rings and J-pivotal monomials. *J. Math. Sci.* **1** (1966), 49–51.

[43] L. P. Belluce and S. K. Jain, Prime rings with a one-sided ideal satisfying a polynomial identity. *Pacif. J. Math.* **24** (1968), 421–424.

[44] J. Bergen, Automorphisms with unipotent values. *Rend. Circ. Mat. Palermo* **31** (1982), 226–232.

[45] J. Bergen, Derivations in prime rings. *Canad. Math. Bull.* **26** (1983), 267–270.

[46] J. Bergen, Automorphic-differential identities in rings. *Proc. Amer. Math. Soc.* **106** (1989), 297–305.

[47] J. Bergen and I. N. Herstein, The algebraic hypercenter and some applications. *J. Algebra* **85** (1983), 217–242.

[48] J. Bergen, I. N. Herstein, and J. W. Kerr, Lie ideals and derivations of prime rings. *J. Algebra* **71** (1981), 259–267.

[49] G. M. Bergman, Modules over coproducts of rings. *Trans. Amer. Math. Soc.* **200** (1974), 1–32.

[50] G. M. Bergman, Rational identities in division rings, I. *J. Algebra* **43** (1976), 252–266.

[51] G. M. Bergman, Rational identities in division rings, II. *J. Algebra* **43** (1976), 267–297.

[52] G. M. Bergman, The diamond lemma. *Adv. Math.* **29** (2) (1978), 178–218.

[53] G. M. Bergman and I. M. Isaacs, Rings with fixed-point-free group actions. *Proc. London Math. Soc.* **27** (1973), 69–87.

[54] W. D. Blair, Remarks on primitive rings with nonzero socles. *Comm. Algebra* **8** (1980), 623–634.

[55] P. Blau. *Lie isomorphisms of prime rings satisfying S_4*, PhD thesis, Univ. of Massachusetts, 1996.

[56] L. A. Bokut, Unsolvability of the equality problem and subalgebras of finitely presented Lie algebras. *Math. USSR Izvestia* **6** (6) (1972), 1153–1199.

[57] L. A. Bokut, Embedding into simple associative algebras. *Algebra and Logic* **15** (2) (1976), 117–142.

[58] L. A. Bokut, Grebner-Širshov bases of Lie algebras. In *Proceedings of Int. Conf. "Algebra and Analysis", Kazan*, 1994, 114–115.

[59] M. Brešar, A note on derivations. *Math. J. Okayama Univ.* **32** (1990), 83–88.

[60] M. Brešar, Semiderivations of prime rings. *Proc. Amer. Math. Soc.* **108** (1990), 859–860.

[61] M. Brešar, On a generalization of the notion of centralizing mappings. *Proc. Amer. Math. Soc.* **114** (1992), 641–649.

[62] M. Brešar, Centralizing mappings and derivations in prime rings. *J. Algebra* **156** (1993), 385–394.

[63] M. Brešar, Commuting traces of biadditive mappings, commutativity preserving mappings, and Lie mappings. *Trans. Amer. Math. Soc.* **335** (1993), 525–546.

[64] M. Brešar, On certain pairs of automorphisms of rings. *J. Austral. Math. Soc. (Ser. A)* **54** (1993), 29–38.

[65] M. Brešar, On skew-commuting mappings of rings. *Bull. Austral. Math. Soc.* **47** (1993), 291–296.

[66] M. Brešar, On certain pairs of functions of semiprime rings. *Proc. Amer. Math. Soc.* **120** (1994), 709–713.

[67] M. Brešar, Functional identities of degree two. *J. Algebra* **172** (1995), 690–720.

[68] M. Brešar, On generalized biderivations and related maps. *J. Algebra* **172** (1995), 764–786.

[69] M. Brešar, W. S. Martindale 3rd, and C. R. Miers, Centralizing maps in prime rings with involution. *J. Algebra* **161** (1993), 342–357.

[70] M. Brešar, W. S. Martindale 3rd, and C. R. Miers, On some identities in prime rings with involution. *Comm. Algebra* **21** (1993), 4679–4697.

[71] M. Brešar and J. Vukman, On left derivations and related mappings. *Proc. Amer. Math. Soc.* **110** (1990), 7–16.

[72] L. Carini and A. Giambruno, Lie ideals and nil derivations. *Bolletino U.M.I.* **6** (1985), 497–503.

[73] J.-C. Chang, On semiderivations of prime rings. *Chinese J. Math.* **12** (1984), 255–262.

[74] J.-C. Chang, On fixed power central (α, β)-derivations. *Bull. Inst. Math. Acad. Sinica* **15** (1987), 163–178.

[75] J.-C. Chang, Lie ideals and derivations in prime rings. *Bull. Inst. Math. Acad. Sinica* **17** (1989), 109–114.

[76] J.-C. Chang, A note on (α, β)-derivations. *Chinese J. Math.* **19** (1991), 277–285.

[77] J.-C. Chang, On (α, β)-derivations of prime rings. *Chinese J. Math.* **22** (1994), 21–30.

[78] M. A. Chebotar, On a composition of derivations of prime rings. *Moscow Univ. Math. Bull.* **50** (2) (1995), 22–25.

[79] M. A. Chebotar, On certain subrings and ideals of prime rings. In *Proceedings of the Tainan-Moscow Algebra Workshop*, Walter de Gruyter, to appear.

[80] C.-L. Chuang, On invariant additive subgroups. *Israel J. Math.* **57** (1987), 116–128.

[81] C.-L. Chuang, *GPI*'s having coefficients in Utumi quotient rings. *Proc. Amer. Math. Soc.* **103** (1988), 723–728.

[82] C.-L. Chuang, $*$-Differential identities of prime rings with involution. *Trans. Amer. Math. Soc.* **316** (1989), 251–279.

[83] C.-L. Chuang, On nilpotent derivations of prime rings. *Proc. Amer. Math. Soc.* **107** (1989), 67–71.

[84] C.-L. Chuang, On compositions of derivations of prime rings. *Proc. Amer. Math. Soc.* **180** (1990), 647–652.

[85] C.-L. Chuang, On the structure of semiderivations in prime rings. *Proc. Amer. Math. Soc.* **108** (1990), 867–869.

[86] C.-L. Chuang, Differential identities with automorphisms and antiautomorphisms, I. *J. Algebra* **149** (1992), 371–404.

[87] C.-L. Chuang, A short proof of Martindale's theorem on *GPI*s. *J. Algebra* **151** (1992), 156–159.

[88] C.-L. Chuang, Differential identities with automorphisms and antiautomorphisms, II. *J. Algebra* **160** (1993), 130–171.

[89] C.-L. Chuang, P. H. Lee, and T. C. Lee, Derivations with central values on powers of symmetric elements. *J. Algebra* **161** (1993), 237–244.

[90] L. O. Chung and J. Luh, On semicommuting automorphisms of rings. *Canad. Math. Bull.* **21** (1978), 13–16.

[91] L. O. Chung and J. Luh, Semiprime rings with nilpotent derivations. *Canad. Math. Bull.* **24** (1981), 415–421.

[92] L. O. Chung and J. Luh, Derivations of higher order and commutativity of rings. *Pacif. J. Math.* **99** (1982), 317–326.

[93] L. O. Chung and J. Luh, Nilpotency of derivations on an ideal. *Proc. Amer. Math. Soc.* **90** (1984), 211–214.

[94] P. M. Cohn, On the free product of associative rings. *Math. Z.* **71** (1959), 380–398.

[95] P. M. Cohn, On the free product of associative rings, II. *Math. Z.* **73** (1960), 433–456.

[96] P. M. Cohn, On the free product of associative rings, III. *J. Algebra* **8** (1968), 376–383.

[97] P. C. Desmarais and W. S. Martindale 3rd, Primitive rings with involution and pivotal monomials. *Israel J. Math.* **22** (1975), 118–126.

[98] P. C. Desmarais and W. S. Martindale 3rd, Generalized rational identities and rings with involution. *Israel J. Math.* **36** (1980), 187–192.

[99] M. P. Drazin, A generalization of polynomial identities in rings. *Proc. Amer. Math. Soc.* **8** (1957), 352–361.

[100] T. S. Erickson, The Lie structure in prime rings with involution. *J. Algebra* **21** (1972), 523–534.

[101] T. S. Erickson, W. S. Martindale, and J. Osborn, Prime nonassociative algebras. *Pacif. J. Math.* **60** (1975), 49–63.

[102] B. Felzenswalb, Derivations in prime rings. *Proc. Amer. Math. Soc.* **84** (1982), 16–20.

[103] B. Felzenswalb and A. Giambruno, A commutativity theorem for rings with derivations. *Pacif. J. Math.* **102** (1982), 41–45.

[104] A. L. Fernándes, E. R. García, and E. C. Sánchez, Structure theorem for prime rings satisfying a generalized identity. *Comm. Algebra* **22** (1994), 1729–1740.

[105] E. Formanek, Central polynomials for matrix rings. *J. Algebra* **23** (1972), 129–132.

[106] G. M. Gabera and P. A. Rodrigues, A characterization of the center of a nondegenerate Jordan algebra. *Comm. Algebra* **21** (1993), 359–369.

[107] A. Giambruno and I. N. Herstein, Derivations with nilpotent values. *Rend. Circ. Mat. Palermo* **30** (1981), 199–206.

[108] I. Z. Golubchik and A. V. Mikhalev, Generalized group identities in classical groups. *Russian Math. Surveys* **35** (6) (1980), 155–156.

[109] I. Z. Golubchik and A. V. Mikhalev, Generalized group identities in classical groups. *Zap. nauch. semin. LOMI AN SSSR* **114** (1982), 96–119 (Russian).

[110] P. Grzeszczuk, On nilpotent derivations of semiprime rings. *J. Algebra* **149** (1992), 313–321.

[111] N. I. Guseva, Semiprime algebras with one-sided ideal that satisfies a polynomial identity. *Russian Math. Surveys* **32** (3) (1977), 155–156.

[112] N. I. Guseva, Semiprime algebras with one-sided ideal that satisfies a polynomial identity. *Izvestia Vuz. Mat.* **23** (4) (1979), 3–13.

[113] I. N. Herstein, Lie and Jordan structure in simple, associative rings. *Bull. Amer. Math. Soc.* **67** (1961), 517–531.

[114] I. N. Herstein, Special simple rings with involution. *J. Algebra* **6** (1967), 369–375.

[115] I. N. Herstein. *Noncommutative rings*, The Carus Math. Monographs, N 15. Math. Association of America, 1968.

[116] I. N. Herstein. *Topics in ring theory.* The University of Chicago Press, 1969.

[117] I. N. Herstein, On the Lie structure of an associative ring. *J. Algebra* **14** (1970), 561–571.

[118] I. N. Herstein. *Rings with involution*, Chicago Lectures in Math. The Universtity Chicago Press, 1976.

[119] I. N. Herstein, A note on derivations. *Canad. Math. Bull.* **21** (1978), 369–370.

[120] I. N. Herstein, Center-like elements in prime rings. *J. Algebra* **60** (1979), 567–574.

[121] I. N. Herstein, A note on derivations, II. *Canad. Math. Bull.* **4** (1979), 509–511.

[122] I. N. Herstein, A theorem on derivations of prime rings with involution. *Canad. Math. Bull.* **34** (1982), 356–369.

[123] I. N. Herstein and E. Kleinfeld, Lie mappings in characteristic 2. *Pacif. J. Math.* **10** (1960), 843–852.

[124] I. N. Herstein and S. Montgomery, Invertible and regular elements in rings with involution. *J. Algebra* **25** (1973), 390–400.

[125] I. N. Herstein and L. Small, Some comments on prime rings. *J. Algebra* **60** (1979), 223–228.

[126] Y. Hirano, A. Kaya, and H. Tominaga, On a theorem of Mayne. *Math. J. Okayama Univ.* **25** (1983), 125–132.

[127] Y. Hirano, H. Tominaga, and A. Trzepizur, On a theorem of Posner. *Math. J. Okayama Univ.* **27** (1985), 25–32.

[128] M. Hongan, A generalization of a theorem of Posner. *Math. J. Okayama Univ.* **33** (1991), 97–101.

[129] R. A. Howland, Lie isomorphisms of derived rings of simple rings. *Trans. Amer. Math. Soc.* **145** (1969), 383–396.

[130] L. Hua, A theorem on matrices over an sfield and its applications. *J. Chinese Math. Soc.* **1** (1951), 110–163.

[131] N. Jacobson, Abstract derivations and Lie algebras. *Trans. Amer. Math. Soc.* **42** (1937), 206–224.

[132] N. Jacobson. *Lie Algebras.* Dover, New York, 1962.

[133] N. Jacobson. *Structure of Rings.* Amer. Math. Soc. Colloquium Publ., Providence, 1964.

[134] S. K. Jain, Polynomial rings with pivotal monomial. *Proc. Amer. Math. Soc.* **17** (1966), 942–945.

[135] S. K. Jain, Prime rings having one-sided ideal with polynomial identity coincide with special Johnson rings. *J. Algebra* **19** (1971), 125–130.

[136] S. K. Jain and S. Singh, Rings having one-sided ideals satisfying a polynomial identity. *Arch. Math. (Basel)* **20** (1969), 17–23.

[137] I. Kaplansky, Rings with a polynomial identity. *Bull. Amer. Math. Soc.* **54** (1948), 575–580.

[138] A. Kaya, A theorem on semi-centralizing derivations of prime rings. *Math. J. Okayama Univ.* **27** (1985), 11–12.

[139] A. Kaya, Semi-centralizing derivations in prime rings. *Doğa Mat.* **11** (1987), 100–105.

[140] A. Kaya and C. Koc, Semicentralizing automorphisms of prime rings. *Acta Math. Acad. Sci. Hungar.* **38** (1981), 53–55.

[141] W. F. Ke, On derivations of prime rings of characteristic 2. *Chinese J. Math.* **13** (1985), 273–290.

[142] V. K. Khachenko. *Automorphisms and Derivations of Associative Rings*, Mathematics and Its Applications (Soviet Series). Kluwer Academic Publishers, Dordrecht / Boston / London, 1991.

[143] V. K. Kharchenko, Generalized identities with automorphisms. *Algebra and Logic* **14** (2) (1975), 132–148.

[144] V. K. Kharchenko, Generalized identities with automorphisms of associative rings with unity. *Algebra i Logika* **14** (6) (1975), 681–696 (Russian).

[145] V. K. Kharchenko, Ring identities with automorphisms. *Siberian Math. J.* **17** (2) (1976), 446–467 (Russian).

[146] V. K. Kharchenko, Differential identities of prime rings. *Algebra and Logic* **17** (2) (1978), 155–168.

[147] V. K. Kharchenko, Differential identities of semiprime rings. *Algebra and Logic* **18** (1) (1979), 58–80.

[148] V. K. Kharchenko, Actions of groups and Lie algebras on noncommutative rings. *Russian Math. Surveys* **35** (2) (1980), 77–104.

[149] V. K. Kharchenko, Skew derivations of semiprime rings. *Siberian Math. J.* **32** (1991), 1045–1051.

[150] V. K. Kharchenko and A. Z. Popov, Skew derivations of prime rings. *Comm. Algebra* **20** (1992), 3321–3345.

[151] A. Kovacs, The n-center of a ring. *J. Algebra* **40** (1976), 107–124.

[152] A. Kovacs, On derivations in prime rings and a question of Herstein. *Canad. Math. Bull.* **22** (1979), 339–344.

[153] J. Krempa and J. Matczuk, On the composition of derivations. *Rend. Circ. Mat. Palermo* **33** (1984), 441–455.

[154] L. A. Lagutina, On Lie automorphisms of simple associative algebras with involution. *Russian Math. Surveys* **47** (6) (1992), 219–220.

[155] J. Lambek. *Lectures on Rings and Modules.* Waltham, Mass.: Blaisdell, 1966.

[156] C. Lanski, Conjugates in prime rings. *Trans. Amer. Math. Soc.* **154** (1971), 185–192.

[157] C. Lanski, Lie ideals and derivations in rings with involution. *Pacif. J. Math.* **69** (1977), 449–460.

[158] C. Lanski, Invariant submodules in semi-prime rings. *Comm. Algebra* **6** (1978), 75–96.

[159] C. Lanski, Differential identities in prime rings with involution. *Trans. Amer. Math. Soc.* **291** (1985), 765–787.

[160] C. Lanski, Minimal differential identities in prime rings. *Israel J. Math.* **56** (1986), 231–246.

[161] C. Lanski, A note on *GPI*'s and their coefficients. *Proc. Amer. Math. Soc.* **98** (1986), 17–19.

[162] C. Lanski, Derivations which are algebraic on subsets of prime rings. *Comm. Algebra* **15** (1987), 1255–1287.

[163] C. Lanski, Correction to "Differential identities in prime rings with involution". *Trans. Amer. Math. Soc.* **309** (1988), 857–859.

[164] C. Lanski, Differential identities, Lie ideals, and Posner's theorems. *Pacif. J. Math.* **134** (1988), 275–297.

[165] C. Lanski, Derivations with nilpotent values on Lie ideals. *Proc. Amer. Math. Soc.* **98** (1990), 17–19.

[166] C. Lanski, Minimal $*$-differential identities in prime rings. *J. Algebra* **133** (1990), 472–489.

[167] C. Lanski, Derivations nilpotent on subsets of primes rings. *Comm. Algebra* **20** (1992), 1427–1446.

[168] C. Lanski, Differential identities in prime rings, Kharchenko's theorem, and applications. *Contemporary Math.* **124** (1992), 111–128.

[169] C. Lanski, Lie ideals and central polynomials with derivations. *Canad. J. Math.* **44** (1992), 553–560.

[170] C. Lanski, Quadratic central polynomials with derivations and involution. *Pacif. J. Math.* **155** (1992), 111–127.

[171] C. Lanski, An Engel condition with derivation. *Proc. Amer. Math. Soc.* **118** (1993), 731–734.

[172] C. Lanski, Derivations with nilpotent values on left ideals. *Comm. Algebra* **22** (1994), 1305–1320.

[173] P. H. Lee and T. K. Lee, On derivations of prime rings. *Chinese J. Math.* **9** (1981), 107–110.

[174] P. H. Lee and T. K. Lee, Lie ideals of prime rings with derivations. *Bull. Inst. Math. Acad. Sinica* **11** (1983), 75–80.

[175] P. H. Lee and T. K. Lee, Derivations centralizing symmetric or skew elements. *Bull. Inst. Math. Acad. Sinica* **14** (1986), 249–256.

[176] P. H. Lee and T. K. Lee, Note on nilpotent derivations. *Proc. Amer. Math. Soc.* **98** (1986), 31–32.

[177] T. K. Lee, Derivations of prime rings with involution, I. *Chinese J. Math.* **13** (1985), 179–186.

[178] T. K. Lee, Derivations of prime rings with involution, II. *Bull. Inst. Math. Acad. Sinica* **14** (1986), 365–375.

[179] T. K. Lee, On derivations. *Bull. Inst. Math. Acad. Sinica* **18** (1990), 307–320.

[180] T. K. Lee, Powers of skew and symmetric elements under a derivation. *Bull. Inst. Math. Acad. Sinica* **18** (1990), 307–320.

[181] T. K. Lee, Semiprime rings with differential identities. *Bull. Inst. Math. Acad. Sinica* **20** (1992), 27–38.

[182] T. K. Lee, Derivations with invertible values on a multilinear polynomial. *Proc. Amer. Math. Soc.* **119** (1993), 1077–1083.

[183] T. K. Lee, Left annihilators characterized by GPI's. *Proc. Amer. Math. Soc., to appear.*

[184] T. K. Lee, Commuting additive mappings in semiprime rings. *Bull. Inst. Math. Acad. Sinica, to appear.*

[185] A. Leroy, Derivees logarithmiques pour une S-dérivation algébrique. *Comm. Algebra* **13** (1985), 85–100.

[186] A. Leroy, (S)-dérivation algébrique sur les corps gauches et sur les anneaux premiers. *Comm. Algebra* **14** (1986), 1473–1479.

[187] A. Leroy and J. Matzuk, Dérivations et automorphismes algébrique d'aneaux premiers. *Comm. Algebra* **13** (1985), 1245–1266.

[188] A. Leroy and J. Matzuk, Quelques remarques à propos des S-derivations. *Comm. Algebra* **13** (1985), 1229–1244.

[189] A. I. Lichtman, The primitivity of free products of associative algebras. *J. Algebra* **54** (1978), 153–158.

[190] A. I. Lichtman and W. S. Martindale 3rd, The normal closure of the coproduct of domains over a division ring. *Comm. Algebra* **13** (1985), 1643–1664.

[191] J. S. Lin, On derivations of prime rings with involution. *Chinese J. Math.* **14** (1986), 37–51.

[192] J. S. Lin, Derivations with invertible values in semiprime rings with involution. *Chinese J. Math.* **18** (1990), 175–184.

[193] J. S. Lin and C. K. Wong, On the skew hypercenter of a ring. *Chinese J. Math.* **18** (1990), 257–271.

[194] D. E. Littlewood, Identical relations satisfied in an algebra. *Proc. London Math. Soc.* **32** (1931), 312–320.

[195] J. Luh, A note on commuting automorphisms of rings. *Amer. Math. Monthly* **77** (1970), 61–62.

[196] A. I. Maltsev. *Algebraic systems.* Springer-Verlag, Berlin–New York, 1973.

[197] A. Mansoor, Lie and Jordan ideals in prime rings with derivations. *Proc. Amer. Math. Soc.* **66** (1976), 275–278.

[198] A. Mansoor, On a theorem of Posner. *Proc. Amer. Math. Soc.* **66** (1977), 13–16.

[199] Z. Maoulaoui and A. Page, Automorphismes algébriques. *Comm. Algebra* **10** (1982), 1497–1515.

[200] W. S. Martindale 3rd, Primitive algebras with involution. *Pacif. J. Math.* **11** (1961), 1431–1441.

[201] W. S. Martindale 3rd, Lie isomorphisms of primitive rings. *Proc. Amer. Math. Soc.* **14** (1963), 909–916.

[202] W. S. Martindale 3rd, Lie derivations of primitive rings. *Michigan Math. J.* **11** (1964), 183–187.

[203] W. S. Martindale 3rd, Lie isomorphisms of prime rings. *Trans. Amer. Math. Soc.* **142** (1969), 437–455.

[204] W. S. Martindale 3rd, Lie isomorphisms of simple rings. *J. London Math. Soc.* **44** (1969), 213–221.

[205] W. S. Martindale 3rd, Prime rings satisfying a generalized polynomial identity. *J. Algebra* **12** (1969), 576–584.

[206] W. S. Martindale 3rd, Rings with involution and polynomial identities. *J. Algebra* **11** (1969), 186–194.

[207] W. S. Martindale 3rd, Primitive rings with involution whose symmetric elements satisfy a generalized polynomial identity. *Proc. Amer. Math. Soc.* **24** (1970), 508–511.

[208] W. S. Martindale 3rd, Prime rings with involution and generalized polynomial identities. *J. Algebra* **22** (1972), 502–516.

[209] W. S. Martindale 3rd, On semiprime *PI* rings. *Proc. Amer. Math. Soc.* **40** (1973), 365–369.

[210] W. S. Martindale 3rd, A note on Lie isomorphisms. *Canad. Math. Bull.* **17** (1974), 243–245.

[211] W. S. Martindale 3rd, Lie isomorphisms of the skew elements of a simple ring with involution. *J. Algebra* **36** (1975), 408–415.

[212] W. S. Martindale 3rd, Lie isomorphisms of the skew elements of a prime ring with involution. *Comm. Algebra* **4** (1976), 927–977.

[213] W. S. Martindale 3rd, Lie and Jordan mappings. *Contemporary Math.* **13** (1982), 173–177.

[214] W. S. Martindale 3rd, Lectures at Jilin University. *Univ. of Massachusetts at Amherst, Department of Math. and Statistic* (1986).

[215] W. S. Martindale 3rd, The normal closure of the coproduct of rings over a division ring. *Trans. Amer. Math. Soc.* **293** (1986), 303–317.

[216] W. S. Martindale 3rd, X-inner derivations of coproducts: Ring theory. *in "Israel Math. Conf. Proc.", Weizmann* (1989), 234–241.

[217] W. S. Martindale 3rd, The symmetric ring of quotients of the coproduct of rings. *J. Algebra* **143** (1991), 295–306.

[218] W. S. Martindale 3rd and C. R. Miers, On the iterates of derivations of prime rings. *Pacif. J. Math.* **104** (1983), 179–190.

[219] W. S. Martindale 3rd and C. R. Miers, Herstein's Lie theory revisited. *J. Algebra* **98** (1986), 14–37.

[220] W. S. Martindale 3rd and C. R. Miers, Nilpotency and generalized Lie ideals. *J. Algebra* **127** (1989), 244–254.

[221] W. S. Martindale 3rd and C. R. Miers, Nilpotent inner derivations of the skew elements of prime rings with involution. *Canad. J. Math.* **43** (1991), 1045–1054.

[222] W. S. Martindale 3rd and C. R. Miers, Generalized Lie ideals in $*$-prime rings. *J. Algebra* **152** (1992), 94–115.

[223] W. S. Martindale 3rd and S. Montgomery, The normal closure of coproducts of domains. *J. Algebra* **82** (1983), 1–17.

[224] J. H. Mayne, Centralizing automorphisms of prime rings. *Canad. Math. Bull.* **19** (1976), 113–115.

[225] J. H. Mayne, Ideals and centralizing mappings in prime rings. *Proc. Amer. Math. Soc.* **86** (1982), 211–212.

[226] J. H. Mayne, Centralizing mappings of prime rings. *Canad. Math. Bull.* **27** (1984), 122–126.

[227] J. H. Mayne, Centralizing automorphisms of Lie ideals in prime rings. *Canad. Math. Bull.* **35** (1992), 510–514.

[228] A. V. Mikhalev, Orthogonally complete many-sorted systems. *Doklady Akad Nauk SSSR* **289** (1986), 1304–1308 (Russian).

[229] A. Milinski, Actions of pointed Hopf algebras on prime algebras. *Comm. Algebra* **23** (1995), 313–333.

[230] S. Montgomery, A structure theorem and a positive-definiteness condition in rings with involution. *J. `Algebra* **43** (1976), 181–192.

[231] S. Montgomery. *Fixed Rings of Finite Automorphism Groups of Associative Rings*, Lecture Notes in Math., 818. Springer-Verlag, Berlin–New York, 1980.

[232] S. Montgomery. *Hopf Algebras and Their Actions on Rings*, Regional Conference Series in Math., 82. Amer. Math. Soc., Providence, Rhode Island, 1993.

[233] A. Ouarit, Identités auto-différentielles d'aneaux semi-premiers. *C. R. Acad. Sci. Paris, Serie I* **314** (1992), 173–176.

[234] J.-L. Pascaud, J. Valette, and J.-M. Goursaud. *Sur les travaux de V. K. Kharchenko*, volume 924 of *Lecture Notes in Math.*, 322–355. Springer, Berlin-New York, 1982.

[235] D. S. Passman, Group rings satisfying a polynomial identity, II. *Paicf. J. Math.* **39** (1971), 425–438.

[236] D. S. Passman, Computing the symmetric ring of quotients. *J. Algebra* **105** (1987), 207–235.

[237] A. E. Pentus, An ideal of generalized identities with involution of an $n \times n$-matrix ring over a finite field. *Russian Math. Surveys* **47** (1992), 187–188.

[238] A. E. Pentus, A structure of a T-ideal of generalized identities of primitive algebras with involution over a field. *Russian Math. Surveys* **47** (1992), 227–228.

[239] A. E. Pentus, A T-ideal of generalized identities for a class of primitive algebras with involution. *Fundamental and Applied Math.* **1** (1995), 255–262 (Russian).

[240] A. Z. Popov, Derivations of prime rings. *Algebra and Logic* **22** (1) (1983), 58–36.

[241] E. Posner, Derivations in prime rings. *Proc. Amer. Math. Soc.* **8** (1957), 79–92.

[242] E. Posner, Prime rings satisfying a polynomial identity. *Arch. Math.* **11** (1960), 180–183.

[243] E. Posner and H. Schneider, Hyperplanes and prime rings. *Arch. Math.* **11** (1960), 322–326.

[244] C. Procesi. *Rings with polynomial identities*, Pure and Applied Math. Marcel Dekker, Inc. New York, 1973.

[245] A. Ram, Lie and Jordan structure in prime rings with derivations. *Proc. Amer. Math. Soc.* **41** (1973), 67–74.

[246] Y. P. Razmyslov, A certain problem of Kaplansky. *Izv Acad. Nauk SSSR Ser. Mat.* **37** (1973), 483–501.

[247] Y. P. Razmyslov. *Identities of Algebras and Their Representations.* Nauka, Moscow, 1989.

[248] A. R. Richardson, Equations over a division algebra. *Messenger of Math.* **57** (1928), 1–6.

[249] A. Richoux, A theorem for prime rings. *Proc. Amer. Math. Soc.* **77** (1979), 27–31.

[250] J. D. Rosen, $*$-Generalized polynomial identities of finite dimensional central simple algebras. *Israel J. Math.* **46** (1983), 97–101.

[251] J. D. Rosen, Generalized rational identities and rings with involution. *J. Algebra* **89** (1984), 416–436.

[252] J. D. Rosen and M. P. Rosen, Generalized rational identities of power series rings. *J. Algebra* **103** (1986), 520–526.

[253] M. P. Rosen, Lie isomorphisms of a certain class of prime rings. *J. Algebra* **89** (1984), 291–317.

[254] S. Rosset, A short proof of the Amitsur-Levitzki theorem. *Israel J. Math.* **23** (1976), 187–188.

[255] L. H. Rowen, On rings with central polynomials. *J. Algebra* **31** (1974), 393–426.

[256] L. H. Rowen, Generalized polynomial identities. *J. Algebra* **34** (1975), 458–480.

[257] L. H. Rowen, Structure of rings with involution applied to generalized polynomial identities. *Canad. J. Math.* **27** (1975), 573–584.

[258] L. H. Rowen, Generalized polynomial identities, II. *J. Algebra* **38** (1976), 380–392.

[259] L. H. Rowen, Monomial conditions on rings. *Israel J. Math.* **23** (1976), 19–30.

[260] L. H. Rowen, Generalized polynomial identities, III. *J. Algebra* **46** (1977), 305–314.

[261] L. H. Rowen, Monomial conditions on prime rings. *Israel J. Math.* **27** (1977), 131–149.

[262] L. H. Rowen, Correction to "monomial conditions on prime rings". *Israel J. Math.* **30** (1979), 279–286.

[263] L. H. Rowen. *Polynomial identities in ring theory*, Pure and Applied Math., 84. Harcout Brace Jovanovich, Publishers, 1980.

[264] R. Ruchti, Twisted Hopf algebras. *Comment. Math. Helvetici* **54** (1979), 659–682.

[265] J. B. Skinner. *Generalized polynomial identities*, PhD thesis, Univ. of Massachusetts, 1970.

[266] M. Slater, On simple rings satisfying a type of "restricted" polynomial identity. *J. Algebra* **1** (1964), 347–354.

[267] M. F. Smiley, Remarks on the commutativity of rings. *Proc. Amer. Math. Soc.* **10** (1959), 466–470.

[268] B. Stendström. *Rings of quotients*, Lecture Notes in Math., 237. Springer-Verlag, Berlin–New York, 1971.

[269] G. Swain. *Lie derivations of the skew elements of prime rings with involution*, PhD thesis, Univ. of Massachusetts, 1993.

[270] Y. Utumi, On quotient rings. *Osaka J. Math.* **8** (1956), 1–18.

[271] J. Valette, Automorphismes algébriques et algébre du groupe. *Comm. Algebra* **11** (1983), 461–468.

[272] A. I. Širšov, On Levitzki problem. *Dokl. Akad. Nauk SSSR* **120** (1958), 41–42.

[273] A. I. Širšov, Some algorithmic problems for Lie algebras. *Siberian Math. J.* **3** (2) (1962), 292–296.

[274] J. Vukman, Commuting and centralizing mappings in prime rings. *Proc. Amer. Math. Soc.* **109** (1990), 47–52.

[275] E. A. Whelan, The symmetric ring of quotients of a primitive ring is primitive. *Comm. Algebra* **18** (1990), 615–633.

[276] K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov, and A. I. Shirshov. *Rings That are Nearly Associative.* Academic Press, 1982.

This Page Intentionally Left Blank

Index