An Introduction to Central Simple Algebras and Their Applications to Wireless Communication

Grégory Berhuy
Frédérique Oggier
An Introduction to Central Simple Algebras and Their Applications to Wireless Communication
An Introduction to Central Simple Algebras and Their Applications to Wireless Communication

Grégory Berhuy
Frédérique Oggier

American Mathematical Society
Providence, Rhode Island
Contents

Foreword ....................................................................................... vii

Introduction ................................................................................... 1

Chapter I. Central simple algebras ............................................... 3
  I.1. Preliminaries on \( k \)-algebras ......................................... 3
  I.2. Central simple algebras: the basics ............................... 7
  I.3. Introducing space-time coding .................................. 11
  Exercises ........................................................................... 18

Chapter II. Quaternion algebras .................................................. 21
  II.1. Properties of quaternion algebras ............................. 21
  II.2. Hamilton quaternions .............................................. 27
  II.3. Quaternion algebras based codes ............................ 28
  Exercises ........................................................................... 30

Chapter III. Fundamental results on central simple algebras ........... 31
  III.1. Operations on central simple algebras .................... 31
  III.2. Simple modules .................................................. 35
  III.3. Skolem-Noether’s theorem .................................... 43
  III.4. Wedderburn’s theorem ......................................... 45
  III.5. The centralizer theorem ........................................ 47
  Exercises ........................................................................... 50

Chapter IV. Splitting fields of central simple algebras ................... 53
  IV.1. Splitting fields .................................................... 53
  IV.2. The reduced characteristic polynomial .................... 60
  IV.3. The minimum determinant of a code ....................... 68
  Exercises ........................................................................... 76

Chapter V. The Brauer group of a field ........................................ 79
  V.1. Definition of the Brauer group ................................ 79
  V.2. Brauer equivalence and bimodules ............................ 82
  V.3. Index and exponent ................................................ 91
  Exercises ........................................................................... 98

Chapter VI. Crossed products ...................................................... 101
  VI.1. Definition of crossed products ............................... 101
  VI.2. Some properties of crossed products ....................... 108
  VI.3. Shaping and crossed products based codes ............... 118
  Exercises ........................................................................... 126
Chapter VII. Cyclic algebras .......................................................... 129  
VII.1. Cyclic algebras ............................................................ 129  
VII.2. Central simple algebras over local fields ......................... 137  
VII.3. Central simple algebras over number fields ....................... 139  
VII.4. Cyclic algebras of prime degree over number fields ............. 141  
VII.5. Examples .................................................................. 144  
VII.6. Cyclic algebras and perfect codes .................................... 150  
VII.7. Optimality of some perfect codes ..................................... 156  
Exercises ........................................................................ 163  

Chapter VIII. Central simple algebras of degree 4 ....................... 165  
VIII.1. A theorem of Albert .................................................. 165  
VIII.2. Structure of central simple algebras of degree 4 ................... 168  
VIII.3. Albert’s Theorem ...................................................... 176  
VIII.4. Codes over biquadratic crossed products ......................... 178  
Exercises ........................................................................ 187  

Chapter IX. Central simple algebras with unitary involutions ............ 189  
IX.1. Basic concepts. ......................................................... 189  
IX.2. The corestriction algebra. ............................................ 191  
IX.3. Existence of unitary involutions. .................................... 198  
IX.4. Unitary involutions on crossed products. .......................... 203  
IX.5. Unitary space-time coding ........................................... 209  
Exercises ........................................................................ 228  

Appendix A. Tensor products ..................................................... 231  
A.1. Tensor product of vector spaces ..................................... 231  
A.2. Basic properties of the tensor product ............................... 235  
A.3. Tensor product of \( k \)-algebras ...................................... 242  

Appendix B. A glimpse of number theory ................................. 249  
B.1. Absolute values .......................................................... 249  
B.2. Factorization of ideals in number fields ............................. 253  
B.3. Absolute values on number fields and completion ............... 262  

Appendix C. Complex ideal lattices ......................................... 265  
C.1. Generalities on hermitian lattices .................................... 265  
C.2. Complex ideal lattices .................................................. 266  

Bibliography ........................................................................ 271  
Index .................................................................................. 275
Mathematics continually surprises and delights us with how useful its most abstract branches turn out to be in the real world. Indeed, physicist Eugene Wigner’s memorable phrase¹ “The unreasonable effectiveness of mathematics” captures a critical aspect of this utility. Abstract mathematical ideas often prove to be useful in rather “unreasonable” situations: places where one, a priori, would not expect them at all! For instance, no one who was not actually following the theoretical explorations in multi-antenna wireless communication of the late 1990s would have predicted that division algebras would turn out to be vital in the deployment of multi-antenna communication. Yet, once performance criteria for space-time codes (as coding schemes for multi-antenna environments are called) were developed and phrased as a problem of design of matrices, it was completely natural that division algebras should arise as a solution of the design problem. The fundamental performance criterion ask for $n \times n$ matrices $M_i$ such that the difference of any two of the $M_i$ is of full rank. To anyone who has worked with division algebras, the solution simply leaps out: any division algebra of index $n$ embeds into the $n \times n$ matrices over a suitable field, and the matrices arising from the embedding naturally satisfy this criterion.

But there is more. Not only did division algebras turn out to be the most natural context in which to solve the fundamental design problem above, they also proved to be the correct objects to satisfy various other performance criteria that were developed. For instance, a second, and critical, performance criterion called the coding gain criterion turned out to be naturally satisfied by considering division algebras over number fields and using natural $\mathbb{Z}$-orders within them that arise from rings of integers of maximal subfields. Other criteria (for instance “DMG optimality,” “good shaping,” “information-losslessness” to name just a few) all turned out to be satisfied by considering suitable orders inside suitable division algebras over number fields. Indeed, this exemplifies another phenomenon Wigner describes: after saying that “mathematical concepts turn up in entirely unexpected connections,” he goes on to say that “they often permit an unexpectedly close and accurate description of the phenomena in these connections.” The match between division algebras and the requirement of space-time codes is simply uncanny.

The subject of multi-antenna communication has several unsolved mathematical problems still, for instance, in the area of decoding for large numbers of antennas. Nevertheless, division algebras are already being deployed for practical two-antenna

systems, and codes based on them are now part of various standards of the Institute of Electrical and Electronics Engineers (IEEE). It would behoove a student of mathematics, therefore, to know something about the applicability of division algebras while studying their theory; in parallel, it is vital for a communications engineer working in coding for multiple-antenna wireless to know something about division algebras.

Berhuy and Oggier have written a charming text on division algebras and their application to multiple-antenna wireless communication. There is a wealth of examples here, particularly over number fields and local fields, with explicit calculations, that one does not see in other texts on the subject. By pairing almost every chapter with a discussion of issues from wireless communication, the authors have given a very concrete flavor to the subject of division algebras. The book can be studied profitably not just by a graduate student in mathematics, but also by a mathematically sophisticated coding theorist. I suspect therefore that this book will find wide acceptability in both the mathematics and the space-time coding community and will help cross-communication between the two. I applaud the authors’ efforts behind this very enjoyable book.

B.A. Sethuraman
Northridge, California
42. S. Pumpluen and T. Unger, *Space-time block codes from nonassociative division algebras*, Advances in Mathematics of Communications **5** (2011), no. 3.
45. B. A. Sethuraman, *Division algebras and wireless communication*, Notices of the AMS **57** (2010), no. 11.
Index

$k$-algebra
  center of a, 4
central, 8
definition, 3
morphism, 3
quaternion, 8
simple, 7
split, 9

absolute discriminant, 259
absolute value
  $p$-adic, 262
archimedean, 249
definition, 249
discrete, 250
equivalence, 249
extension, 251
non-archimedean, 249

absolute value
  extension
    totally ramified, 251
    ramification index, 251
    ramified, 251
    residual degree, 251
    unramified, 251

bimodule, 82
Brauer equivalence, 46
Brauer group, 81
relative, 82

canonical involution, 228
centralizer, 31
coboundary, 113
cocycle, 104
codebook, 13
coding gain, 14
coherence interval, 12
coherent, 13
cohomologous cocycles, 113
corestriction, 195
crossed product, 107
cyclic algebra, 130
decomposition group, 261
degree, 46
different ideal, 259
differential modulation, 209
discriminant ideal, 259
diversity, 14
elementary tensor, 233
exponent, 95
fading matrix, 11
Frobenius map, 253
fully diverse code, 14
Goldman element, 86
Hasse symbol, 138
ideal (ramification)
  inert, 255
  ramification index, 255
  ramified, 255
  tamely ramified, 255
  totally ramified, 255
  totally split, 255
  unramified, 255
  wildly ramified, 255
index, 46
information symbol, 12
inner automorphism, 43
involution
  definition of an, 189
  of the first kind, 189
  of the second kind, 189
local parameter, 251
MIMO, 11
module
  definition, 35
  finitely generated, 36
  free, 37
  morphism, 36
  rank, 41
non-coherent, 209
norm of an ideal
absolute norm, 258
relative norm, 258
number field, 253

opposite algebra, 34

place, 249
complex, 262
finite, 262
real, 262

prime ideals
residual degree, 255

ramification groups, 261
rate, 14, 17
reduced characteristic polynomial, 63
reduced norm, 66
reduced trace, 66
residue field, 250
restriction map, 82
ring of integers, 253

Sandwich morphism, 35
semilinear map, 191

simple
module, 39
SNR, 13

space-time codes, 13
splitting field, 53

subalgebra
definition, 3

subfield, 9
submodule, 36

tensor product
of algebras, 5, 243
of vector spaces, 231

trace form, 76

valuation ring, 250
Selected Published Titles in This Series

191 Grégory Berhuy and Frédérique Oggier, An Introduction to Central Simple Algebras and Their Applications to Wireless Communication, 2013
186 Gregory Berkolaiko and Peter Kuchment, Introduction to Quantum Graphs, 2013
185 Patrick Iglesias-Zemmour, Diffeology, 2013
184 Frederick W. Gehring and Kari Hag, The Ubiquitous Quasidisk, 2012
180 Martin W. Liebeck and Gary M. Seitz, Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras, 2012
179 Stephen D. Smith, Subgroup complexes, 2011
178 Helmut Brass and Knut Petras, Quadrature Theory, 2011
176 Peter E. Kloeden and Martin Rasmussen, Nonautonomous Dynamical Systems, 2011
175 Warwick de Launey and Dane Flannery, Algebraic Design Theory, 2011
174 Lawrence S. Levy and J. Chris Robson, Hereditary Noetherian Prime Rings and Idealizers, 2011
173 Sariel Har-Peled, Geometric Approximation Algorithms, 2011
171 Leonid Pastur and Mariya Shcherbina, Eigenvalue Distribution of Large Random Matrices, 2011
170 Kevin Costello, Renormalization and Effective Field Theory, 2011
169 Robert R. Bruner and J. P. C. Greenlees, Connective Real K-Theory of Finite Groups, 2010
168 Michiel Hazewinkel, Nadiya Gubareni, and V. V. Kirichenko, Algebras, Rings and Modules, 2010
167 Michael Gekhtman, Michael Shapiro, and Alek Vainshtein, Cluster Algebras and Poisson Geometry, 2010
166 Kyung Bai Lee and Frank Raymond, Seifert Fiberings, 2010
165 Fuensanta Andrade-Vaillo, José M. Mazón, Julio D. Rossi, and J. Julián Toledo-Melero, Nonlocal Diffusion Problems, 2010
164 Vladimir I. Bogachev, Differentiable Measures and the Malliavin Calculus, 2010
162 Vladimir Maz’ya and Jürgen Rossmann, Elliptic Equations in Polyhedral Domains, 2010
161 Kanishka Perera, Ravi P. Agarwal, and Donal O’Regan, Morse Theoretic Aspects of p-Laplacian Type Operators, 2010
160 Alexander S. Kechris, Global Aspects of Ergodic Group Actions, 2010
159 Matthew Baker and Robert Rumely, Potential Theory and Dynamics on the Berkovich Projective Line, 2010

For a complete list of titles in this series, visit the AMS Bookstore at www.ams.org/bookstore/survseries/.
Central simple algebras arise naturally in many areas of mathematics. They are closely connected with ring theory, but are also important in representation theory, algebraic geometry and number theory.

Recently, surprising applications of the theory of central simple algebras have arisen in the context of coding for wireless communication. The exposition in the book takes advantage of this serendipity, presenting an introduction to the theory of central simple algebras intertwined with its applications to coding theory. Many results or constructions from the standard theory are presented in classical form, but with a focus on explicit techniques and examples, often from coding theory.

Topics covered include quaternion algebras, splitting fields, the Skolem-Noether Theorem, the Brauer group, crossed products, cyclic algebras and algebras with a unitary involution. Code constructions give the opportunity for many examples and explicit computations.

This book provides an introduction to the theory of central algebras accessible to graduate students, while also presenting topics in coding theory for wireless communication for a mathematical audience. It is also suitable for coding theorists interested in learning how division algebras may be useful for coding in wireless communication.

For additional information and updates on this book, visit [www.ams.org/bookpages/surv-191](http://www.ams.org/bookpages/surv-191)