Mathematical Surveys and Monographs

Volume 191

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

Grégory Berhuy
Frédérique Oggier

American Mathematical Society

http://dx.doi.org/10.1090/surv/191

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

Mathematical Surveys and Monographs

Volume 191

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

Grégory Berhuy
Frédérique Oggier

American Mathematical Society
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 12E15; Secondary 11T71, 16W10.

For additional information and updates on this book, visit
www.ams.org/bookpages/surv-191

Library of Congress Cataloging-in-Publication Data

Berhuy, Grégory.
An introduction to central simple algebras and their applications to wireless communications / Grégory Berhuy, Frédérique Oggier.
pages cm. – (Mathematical surveys and monographs ; volume 191)
Includes bibliographical references and index.
ISBN 978-0-8218-4937-8 (alk. paper)
1. Division algebras. 2. Skew fields. I. Oggier, Frédérique. II. Title.

QA247.45.B47 2013
512′.3–dc23 2013009629

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at `http://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 18 17 16 15 14 13

Contents

Foreword

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 phrase[1] "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

[1] Eugene P. Wigner, The unreasonable effectiveness of mathematics in the natural sciences, Comm. Pure Appl. Math., **13** Feb. 1960, 1–14

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

Bibliography

1. S.M. Alamouti, *A simple transmit diversity technique for wireless communications*, IEEE J. Selected Areas Communications **16** (1998), 1451–1458.
2. A.A. Albert, *Structure of Algebras*, A.M.S. Coll.Pub., vol. 24, AMS, 1939.
3. S.A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972), no. 4, 408–420.
4. E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, *New algebraic constructions of rotated $\mathbb{Z}^n$–lattice constellations for the Rayleigh fading channel*, IEEE Transactions on Information Theory **50** (2004), no. 4.
5. J.-C. Belfiore and G. Rekaya, *Quaternionic lattices for space-time coding*, Proceedings of IEEE Information Theory Workshop (ITW), Paris (2003).
6. J.-C. Belfiore, G. Rekaya, and E. Viterbo, *The Golden code: A 2×2 full rate space-time code with non vanishing determinants*, IEEE Trans. on Inf. Theory **51** (2005), no. 4.
7. G. Berhuy, *Algebraic space-time codes based on division algebras with a unitary involution*, (2012), Preprint. Available from `http://www-fourier.ujf-grenoble.fr/~berhuy/fichiers/unitarycodes.pdf`.
8. G. Berhuy and F. Oggier, *Space-time codes from crossed product algebras of degree 4*, Proceedings of Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci **4851** (2007), 90–99.
9. ———, *On the existence of perfect space-time codes*, IEEE Transactions on Information Theory **55** (2009), no. 5, 2078–2082.
10. G. Berhuy and R. Slessor, *Optimality of codes based on crossed product algebras*, (2011), Preprint. Available from `http://www-fourier.ujf-grenoble.fr/~berhuy/Berhuy-Slessor-2209.pdf`.
11. J.W.S. Cassels and A. Frölich, *Algebraic number theory*, Acad. Press, 1967.
12. M. O. Damen, A. Tewfik, and J.-C. Belfiore, *A construction of a space-time code based on number theory*, IEEE Transactions on Information Theory **48** (2002), no. 3.
13. P. Elia, B.A. Sethuraman, and P. V. Kumar, *Perfect space-time codes for any number of antennas*, IEEE Transactions on Information Theory **53** (2007).
14. Jr. G. Forney, R. Gallager, G. Lang, F. Longstaff, and S. Qureshi, *Efficient modulation for band-limited channels*, IEEE Journal on Selected Areas in Communications **2** (1984), no. 5, 632–647.
15. A. Fröhlich and M. Taylor, *Algebraic number theory*, Cambridge University Press, 1991.
16. P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, 2006.
17. D. Haile, *A useful proposition for division algebras of small degree*, Proc. Amer. Math. Soc. **106** (1989), no. 2, 317–319.
18. T. Hanke, *A twisted Laurent series ring that is a noncrossed product*, Israel J. Math. **150** (2005).
19. B. Hassibi and B. Hochwald, *Cayley differential unitary space-time codes*, IEEE Trans. on Information Theory **48** (2002).
20. J. Hiltunen, C. Hollanti, and J. Lahtonen, *Dense full-diversity matrix lattices for four transmit antenna MISO channel*, Proceedings of IEEE International Symposium on Information Theory (ISIT) (2005).
21. B. Hochwald and W. Sweldens, *Differential unitary space time modulation*, IEEE Trans. Commun. **48** (2000).
22. J. G. Huard, B. K. Spearman, and K. S. Williams, *Integral bases for quartic fields with quadratic subfields*, J. Number Theory **51** (1995), no. 1, 87–102. MR1321725 (96a:11115)
23. B. Hughes, *Differential space-time modulation*, IEEE Trans. Inform. Theory **46** (2000).

24. K. Iyanaga, *Class numbers of definite hermitian forms*, J. Math. Soc. Japan **21** (1969).
25. N. Jacobson, *Finite-dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996.
26. G. J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.
27. S. Karmakar and B Sundar Rajan, *High-rate, multi-symbol-decodable STBCs from Clifford algebras*, IEEE Transactions on Information Theory **55** (2009), no. 6.
28. A. W. Knapp, *Advanced algebra*, Cornerstones, Birkhäuser Boston Inc., Boston, MA, 2007, Along with a companion volume ıt Basic algebra.
29. M.A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, Amer. Math. Soc. Coll. Pub., vol. 44, A.M.S, 1998.
30. H. Koch, *Algebraic number theory*, Springer-Verlag,Berlin, 1997.
31. _____, *Number theory: algebraic numbers and functions*, Graduate Studies in Mathematics, vol. 24, A.M.S, 2000.
32. J. Lahtonen, N. Markin, and G. McGuire, *Construction of space-time codes from division algebras with roots of unity as non-norm elements*, IEEE Trans. on Information Theory **54** (2008), no. 11.
33. F. Oggier, *On the optimality of the Golden code*, IEEE Information Theory Workshop (ITW'06) (2006).
34. _____, *Cyclic algebras for noncoherent differential space-time coding*, IEEE Transactions on Information Theory **53 (9)** (2007), 3053–3065.
35. _____, *A survey of algebraic unitary codes*, International Workshop on Coding and Cryptology **5757** (2009), 171–187.
36. F. Oggier, J.-C. Belfiore, and Viterbo E., *Cyclic division algebras: A tool for space-time coding*, Now Publishers Inc., Hanover, MA, USA, 2007.
37. F. Oggier and B. Hassibi, *"an algebraic family of distributed space-time codes for wireless relay networks*, Proceedings of IEEE International Symposium on Information Theory (ISIT) (2006).
38. _____, *Algebraic cayley differential space-time codes*, IEEE Transactions on Information Theory **53** (2007), no. 5.
39. F. Oggier and L. Lequeu, *Families of unitary matrices achieving full diversity*, International Symposium on Information Theory (2005), 1173–1177.
40. F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, *Perfect space-time block codes*, IEEE Trans. Inform. Theory **52** (2006), no. 9.
41. R.S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer-Verlag, New York-Berlin, 1982.
42. S. Pumpluen and T. Unger, *Space-time block codes from nonassociative division algebras*, Advances in Mathematics of Communications **5** (2011), no. 3.
43. P. Ribenboim, *Classical theory of algebraic numbers*, Universitext, Springer, 2001.
44. J.-P. Serre, *Corps locaux (4ème édition)*, Hermann, 1997.
45. B. A. Sethuraman, *Division algebras and wireless communication*, Notices of the AMS **57** (2010), no. 11.
46. B.A. Sethuraman and B. Sundar Rajan, *An algebraic description of orthogonal designs and the uniqueness of the Alamouti code*, Proceedings of GlobCom (2002).
47. _____, *STBC from field extensions of the rational field*, Proceedings of IEEE International Symposium on Information Theory (ISIT), Lausanne (2002).
48. B.A. Sethuraman, B. Sundar Rajan, and V. Shashidhar, *Full-diversity, high-rate space-time block codes from division algebras*, IEEE Transactions on Information Theory **49** (2003).
49. A. Shokrollahi, B. Hassibi, B.M. Hochwald, and W. Sweldens, *Representation theory for high-rate multiple-antenna code design*, IEEE Trans. Information Theory **47** (2001), no. 6.
50. R. Slessor, *Performance of codes based on crossed product algebras*, Ph.D. thesis, School of Mathematics, Univ. of Southampton, May 2011 note = Available from `http://eprints.soton.ac.uk/197309/3.hasCoversheetVersion/Thesis_--_Richard_Slessor.pdf`, OPTannote = annote, 2011.
51. H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, Cambridge University Press, 2001.
52. V. Tarokh, N. Seshadri, and A. Calderbank, *Space-time codes for high data rate wireless communication : Performance criterion and code construction*, IEEE Trans. Inform. Theory **44** (1998), 744–765.

53. The PARI Group, Bordeaux, *PARI/GP, version* `2.3.3`, 2005, available from `http://pari.math.u-bordeaux.fr/`.
54. J.-P. Tignol, *Produits croisés abéliens*, J.of Algebra **70** (1981).
55. T. Unger and N. Markin, *Quadratic forms and space-time block codes from generalized quaternion and biquaternion algebras*, IEEE Trans. on Information Theory **57** (2011), no. 9.
56. R. Vehkalahti, C. Hollanti, J. Lahtonen, and K. Ranto, *On the densest MIMO lattices from cyclic division algebras*, IEEE Transactions on Information Theory **55** (2009), no. 8.
57. S. Vummintala, B. Sundar Rajan, and B.A. Sethuraman, *Information-lossless space-time block codes from crossed-product algebras*, IEEE Trans. Inform. Theory **52** (2006), no. 9.
58. H. Yao and G.W. Wornell, *Achieving the full MIMO diversity-multiplexing frontier with rotation-based space-time codes*, Proceedings of Allerton Conf. on Communication, Control and Computing (2003).

Index

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

187 **Nassif Ghoussoub and Amir Moradifam,** Functional Inequalities: New Perspectives and New Applications, 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

183 **Gershon Kresin and Vladimir Maz'ya,** Maximum Principles and Sharp Constants for Solutions of Elliptic and Parabolic Systems, 2012

182 **Neil A. Watson,** Introduction to Heat Potential Theory, 2012

181 **Graham J. Leuschke and Roger Wiegand,** Cohen-Macaulay Representations, 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

177 **Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov,** Non-commutative Cryptography and Complexity of Group-theoretic Problems, 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

172 **Michael Aschbacher, Richard Lyons, Stephen D. Smith, and Ronald Solomon,** The Classification of Finite Simple Groups, 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 Andreu-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

163 **Bennett Chow, Sun-Chin Chu, David Glickenstein, Christine Guenther, James Isenberg, Tom Ivey, Dan Knopf, Peng Lu, Feng Luo, and Lei Ni,** The Ricci Flow: Techniques and Applications: Part III: Geometric-Analytic Aspects, 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/**.

Photograph courtesy of Gregory Berhuy

Photograph courtesy of A. Datta

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

AMS *on the* Web
www.ams.org

ISBN 978-0-8218-4937-8

9 780821 849378

SURV/191