Author: Ciocanea Teodorescu, I.
Title: Algorithms for finite rings
Issue Date: 2016-06-22

References

[1] M. Agrawal, N. Kayal, and N. Saxena. Primes is in P. *Ann. of Math*, 2:781–793, 2002.

[2] M. Agrawal and N. Saxena. Automorphisms of finite rings and applications to complexity of problems. In Volker Diekert and Bruno Durand, editors, *STACS 2005*, volume 3404 of *Lecture Notes in Computer Science*, pages 1–17. Springer Berlin Heidelberg, 2005.

[3] M. Aguiar. A note on strongly separable algebras. *Boletín de la Academia Nacional de Ciencias (Córdoba, Argentina)*, special issue in honor of Orlando Villamayor(65):51–60, 2000.

[4] V. Arvind, B. Das, and P. Mukhopadhyay. The complexity of black-box ring problems. In *Computing and Combinatorics*, volume 4112 of *Lecture Notes in Computer Science*, pages 126–135. Springer Berlin Heidelberg, 2006.

[5] M. Auslander and O. Goldman. The Brauer group of a commutative ring. *Trans. Am. Math. Soc.*, 97:367–409, 1961.

[6] L. Babai. Graph isomorphism in quasipolynomial time. *preprint*, arXiv:1512.03547, 2015.

[7] H. Bass. *Traces and Euler characteristics.* Lecture Note Series. Cambridge University Press, 1979.

[8] D.J. Bernstein. Factoring into coprimes in essentially linear time. *J. Algorithms*, 54(1):1–30, 2005.

[9] G. Bini and F. Flamini. *Finite Commutative Rings and Their Applications.* The Springer International Series in Engineering and Computer Science. Springer US, 2012.

[10] P.A. Brooksbank and E.M. Luks. Testing isomorphism of modules. *Journal of Algebra*, 320(11):4020–4029, 2008.

[11] P.A. Brooksbank and J.B. Wilson. The module isomorphism problem reconsidered. *Journal of Algebra*, 421:541–559, 2015. Special issue in memory of Ákos Seress.

[12] J.A. Buchmann and H.W. Lenstra. Approximating rings of integers in number fields. *Journal de théorie des nombres de Bordeaux*, 6(2):221–260, 1994.

[13] J.P. Buhler and P. Stevenhagen. *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography.* Mathematical Sciences Research Institute Publications. Cambridge University Press, 2008.

[14] J.F. Buss, G.S. Frandsen, and J.O. Shallit. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences*, 58(3):572–596, 1999.

[15] A. Chistov, G. Ivanyos, and M. Karpinski. Polynomial time algorithms for modules over finite dimensional algebras. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, ISSAC '97, pages 68–74, New York, USA, 1997. ACM.

[16] T.-W.J. Chou and G.E. Collins. Algorithms for the solution of systems of linear diophantine equations. *SIAM Journal on Computing*, 11(4):687–708, 1982.

[17] I. Ciocănea-Teodorescu. The module isomorphism for finite rings and related results. *preprint*, arXiv:1512.08365v1, 2015.

[18] A.M. Cohen, G. Ivanyos, and D.B. Wales. Finding the radical of an algebra of linear transformations. *Journal of Pure and Applied Algebra*, 117-118:177–193, 1997.

[19] H. Cohen. *A Course in Computational Algebraic Number Theory.* Graduate Texts in Mathematics. Springer, 1993.

[20] F. DeMeyer and E. Ingraham. *Separable algebras over commutative rings.* Lecture Notes in Mathematics. Springer, Berlin, 1971.

[21] F.R. DeMeyer. The trace map and separable algebras. *Osaka Journal of Mathematics*, 3(1):7–11, 1966.

[22] L.E. Dickson. Algebras and their arithmetics. *Bulletin of the American Mathematical Society*, 30(5-6):247–257, 1924.

[23] R. Eggermont. *Modellen voor eindige lichamen.* Bachelor thesis. Mathematical Institute, Leiden University, 2009.

[24] S. Endo and Y. Watanabe. On separable algebras over a commutative ring. *Osaka Journal of Mathematics*, 4(2):233–242, 1967.

[25] S. Endo and Y. Watanabe. The centers of semi-simple algebras over a commutative ring. ii. *Nagoya Mathematical Journal*, 39:1–6, 1970.

[26] B. Farb and R.K. Dennis. *Noncommutative Algebra.* Graduate Texts in Mathematics. Springer New York, 2012.

[27] K. Friedl and L. Rónyai. Polynomial time solutions of some problems of computational algebra. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, pages 153–162, New York, NY, USA, 1985. ACM.

[28] T. Fritzsche. The Brauer group of character rings. *Journal of Algebra*, 361(0):37–40, 2012.

[29] G. Ganske and B.R. McDonald. Finite local rings. *Rocky Mountain J. Math.*, 3(4):521–540, 1973.

[30] J.L. Hafner and K.S. McCurley. Asymptotically fast triangulation of matrices over rings. In *Proceedings of the First Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '90, pages 194–200, Philadelphia, PA, USA, 1990. Society for Industrial and Applied Mathematics.

[31] A. Hattori. Semisimple algebras over a commutative ring. *Journal of the Mathematical Society of Japan*, 15(4):404–419, 1963.

[32] A. Hattori. On strongly separable algebras. *Osaka Journal of Mathematics*, 2(2):369–372, 1965.

[33] G. Havas, B.S. Majewski, and K.R. Matthews. Extended GCD and Hermite normal form algorithms via lattice basis reduction. *Experiment. Math.*, 7(2):125–136, 1998.

[34] G. Higman. On a conjecture of Nagata. *Proceedings of the Cambridge Philosophical Society*, 52(Part I), January 1956.

[35] M. Hitz, J. Grabmeier, E. Kaltofen, and V. Weispfenning. *Computer Algebra Handbook: Foundations · Applications · Systems*. SpringerLink : Bücher. Springer Berlin Heidelberg, 2012.

[36] D. F. Holt and S. Rees. Testing modules for irreducibility. *Journal of the Australian Mathematical Society (Series A)*, 57:1–16, 8 1994.

[37] D.F. Holt. The meataxe as a tool in computational group theory. In R.T. Curtis and R.A. Wilson, editors, *The Atlas of Finite Groups - Ten Years on*, pages 74–81. Cambridge University Press, 1998. Cambridge Books Online.

[38] D.F. Holt, B. Eick, and E.A. O'Brien. *Handbook of Computational Group Theory*. Discrete Mathematics and Its Applications. CRC Press, 2005.

[39] G. Ivanyos. Modules and maximum rank matrix completion. Presented at the Combinatorics, Groups, Algorithms, and Complexity Conference, Columbus, Ohio, March 21-25, 2010.

[40] G. Ivanyos, M. Karpinski, Y. Qiao, and M. Santha. Generalized Wong sequences and their applications to Edmonds' problems. *Journal of Computer and System Sciences*, 81(7):1373–1386, 2015.

[41] G. Ivanyos, M. Karpinski, L. Rónyai, and N. Saxena. Trading GRH for algebra: Algorithms for factoring polynomials and related structures. *Math. Comput.*, 81(277):493–531, 2012.

[42] G. Ivanyos, M. Karpinski, and N. Saxena. Deterministic polynomial time algorithms for matrix completion problems. *SIAM J. Comput.*, 39(8):3736–3751, 2010.

[43] G. Ivanyos and K.M. Lux. Treating the exceptional cases of the meataxe. *Experimental Mathematics*, 9(3):373–381, 2000.

[44] G. Ivanyos and L. Rónyai. *Computations in Associative and Lie Algebras*, volume 4 of *Algorithms and Computation in Mathematics*. Springer Berlin Heidelberg, 1999.

[45] G. Ivanyos, L. Rónyai, and J. Schicho. Splitting full matrix algebras over algebraic number fields. *Journal of Algebra*, 354(1):211–223, 2012.

[46] G. Ivanyos, L. Rónyai, and J. Schicho. Improved algorithms for splitting full matrix algebras. *JP Journal of Algebra, Number Theory and Applications*, 28(2):141–156, 2013.

[47] N. Jacobson. *Lie Algebras*. Dover Books on Mathematics Series. Dover, 1979.

[48] N. Jacobson. *Basic algebra II*. Basic Algebra. Dover Publications, Incorporated, 2009.

[49] L. Kadison and A.A. Stolin. *Separability and Hopf algebras*. Algebra and Its Applications: International Conference [on] Algebra and Its Applications, March 25-28, 1999, Ohio University, Athens. American Mathematical Society, 2000.

[50] T. Kanzaki. Special type of separable algebra over a commutative ring. *Proc. Japan Acad.*, 40(10):781–786, 1964.

[51] I. Kaplansky. Rings with a polynomial identity. *Bulletin of the American Mathematical Society*, 54(6):575–580, 1948.

[52] N. Kayal and N. Saxena. On the ring isomorphism and automorphism problems. *IEEE Conference on Computational Complexity*, pages 2–12.

[53] N. Kayal and N. Saxena. Complexity of ring morphism problems. *Computational Complexity*, 15(4):342–390, June 2006.

[54] M.-A. Knus and M. Ojanguren. *Théorie de la descente et algèbres d'Azumaya*. Lecture Notes in Mathematics, Vol. 389. Springer-Verlag, Berlin, 1974.

[55] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer-Verlag New York, Inc., New York, NY, USA, 1987.

[56] T.Y. Lam. *Lectures on Modules and Rings*. Graduate Texts in Mathematics. Springer New York, 1999.

[57] T.Y. Lam. *A First Course in Noncommutative Rings.* Graduate Texts in Mathematics. Springer, 2001.

[58] T.Y. Lam. *Serre's Problem on Projective Modules.* Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2010.

[59] S. Landau. Some remarks on computing the square parts of integers. *Information and Computation*, 78(3):246 – 253, 1988.

[60] S. Lang. *Algebra.* Graduate Texts in Mathematics. Springer New York, 2002.

[61] A.K. Lenstra. Factorization of polynomials. In *Computational methods in number theory*, Mathematical Centre Tracts 154-155, pages 169–198, Amsterdam, 1984. Mathematisch Centrum.

[62] A.K. Lenstra. Integer factoring. *Designs, Codes and Cryptography*, 19(2):101–128, 2000.

[63] A.K. Lenstra, H.W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[64] H.W. Lenstra. *Galois Theory for Schemes.* Course notes available from the server of the Universiteit Leiden Mathematics Department, http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf. Electronic third edition: 2008.

[65] H.W. Lenstra. Finding isomorphisms between finite fields. *Mathematics of Computation*, 56(193):329–347, 1991.

[66] H.W. Lenstra. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc.*, 26:211–244, 1992.

[67] H.W. Lenstra. Flags and lattice basis reduction. In *In Proceedings of the third European congress of mathematics*. Birkhuser, 2001.

[68] H.W. Lenstra. Lattices. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 127–181. Cambridge Univ. Press, Cambridge, 2008.

[69] K.M. Lux and M. Szöke. Computing homomorphism spaces between modules over finite dimensional algebras. *Experiment. Math.*, 12(1):91–98, 2003.

[70] K.M. Lux and M. Szöke. Computing decompositions of modules over finite-dimensional algebras. *Experiment. Math.*, 16(1):1–6, 2007.

[71] G. Marks and M. Schmidmeier. Extensions of simple modules and the converse of Schur's lemma. In *Advances in Ring Theory*, Trends in Mathematics, pages 229–237. Birkhäuser Basel, 2010.

[72] M. Orzech and C. Small. *The Brauer group of commutative rings.* Number v. 11 in Lecture notes in pure and applied mathematics. M. Dekker, 1975.

[73] C.H. Papadimitriou. *Computational Complexity.* Theoretical computer science. Addison-Wesley, 1994.

[74] R. Parker. The computer calculation of modular characters (the meat-axe). *Computational Group Theory*, pages 267–274, 1984.

[75] L. Rónyai. Computing the structure of finite algebras. *J. Symb. Comput.*, 9(3):355–373, March 1990.

[76] J. Rotman. *An Introduction to Homological Algebra.* Universitext. Springer New York, 2008.

[77] L.H. Rowen. *Ring Theory.* Number v. 1 in Pure and Applied Mathematics. Academic Press, 1988.

[78] L.H. Rowen. *Ring Theory.* Number v. 2 in Pure and Applied Mathematics. Academic Press, 1988.

[79] L.H. Rowen. *Graduate Algebra: Noncommutative View.* Graduate Algebra. American Mathematical Society, 2008.

[80] D.J. Saltman. *Lectures on Division Algebras.* Number 94 in CBMS Regional Conference Series. American Mathematical Soc., 1999.

[81] J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, October 1980.

[82] J.P. Serre. *Local Fields.* Graduate Texts in Mathematics. Springer New York, 1995.

[83] M. Staromiejski. Polynomial-time locality tests for finite rings. *Journal of Algebra*, 379(0):441–452, 2013.

[84] A. Storjohann. Computation of Hermite and Smith Normal Forms of Matrices. Master's thesis, Department of Computer Science, University of Waterloo, 1994.

[85] A. Storjohann. Near optimal algorithms for computing smith normal forms of integer matrices. In *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*, ISSAC '96, pages 267–274, New York, NY, USA, 1996. ACM.

[86] A. Storjohann. *Algorithms for Matrix Canonical Forms.* PhD thesis, Department of Computer Science, Swiss Federal Institute of Technology, 2000.

[87] M. Szymik. The Brauer group of Burnside rings. *Journal of Algebra*, 324(9):2589–2593, 2010.

[88] J.A. Wood. Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*, 121:555–575, 1999.

[89] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposium on on Symbolic and Algebraic Computation*, EUROSAM '79, pages 216–226, London, UK, 1979. Springer-Verlag.

Index