Field Theory
Field Theory: General

12Exx

[1] R. D. Baker, G. L. Ebert, K. H. Leung, and Q. Xiang, *A trace conjecture and flag-transitive affine planes*, J. Combin. Theory Ser. A **95** (2001), no. 1, 158–168. MR MR1840482 (2002c:11166)

[2] B. V. Petrenko, *On the product of two primitive elements of maximal subfields of a finite field*, J. Pure Appl. Algebra **178** (2003), no. 3, 297–306. MR MR1953735 (2004b:11165)

[3] ———, *On the sum of two primitive elements of maximal subfields of a finite field*, Finite Fields Appl. **9** (2003), no. 1, 102–116. MR MR1954786 (2003m:12004)

[4] Ruth Schwingel, *The tensor product of polynomials*, Experiment. Math. **8** (1999), no. 4, 395–397. MR MR1737234 (2000j:12004)

[5] Kirby C. Smith and Leon van Wyk, *A concrete matrix field description of some Galois fields*, Linear Algebra Appl. **403** (2005), 159–164. MR MR2140278 (2006b:12002)

Extensions and Galois Theory

12Fxx

[1] Alejandro Adem, Wenfeng Gao, Dikran B. Karagueuzian, and Ján Mináč, *Field theory and the cohomology of some Galois groups*, J. Algebra **235** (2001), no. 2, 608–635. MR MR1805473 (2001m:12011)

[2] Maximilian Albert and Annette Maier, *Additive polynomials for finite groups of Lie type*, 2009.

[3] Bill Allombert, *An efficient algorithm for the computation of Galois automorphisms*, Math. Comp. **73** (2004), no. 245, 359–375 (electronic). MR MR2034127 (2004k:11193)

[4] Johan Bosman, *A polynomial with Galois group* $\mathrm{SL}_2(F_{16})$, LMS J. Comput. Math. **10** (2007), 1461–1570 (electronic). MR MR2365691

[5] Nigel Boston, *Reducing the Fontaine-Mazur conjecture to group theory*, Progress in Galois theory, Dev. Math., vol. 12, Springer, New York, 2005, pp. 39–50. MR MR2148459

[6] Nigel Boston and Charles Leedham-Green, *Explicit computation of Galois p-groups unramified at p*, J. Algebra **256** (2002), no. 2, 402–413. MR MR1939112 (2003k:12004)

[7] Nigel Boston and Harris Nover, *Computing pro-p-Galois groups*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 1–10. MR MR2282911

[8] Nigel Boston and David Perry, *Maximal 2-extensions with restricted ramification*, J. Algebra **232** (2000), no. 2, 664–672. MR MR1792749 (2001k:12005)

[9] Antoine Colin, *Relative resolvents and partition tables in Galois group computations*, Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI) (New York), ACM, 1997, pp. 78–84 (electronic). MR MR1809973 (2001j:12001)

[10] Lassina Dembélé, *A non-solvable Galois extension of Q ramified at 2 only*, C. R. Math. Acad. Sci. Paris **347** (2009), no. 3-4, 111–116. MR MR2538094

[11] Michael Dettweiler, *Galois realizations of classical groups and the middle convolution*, 2006.

[12] Pilar Fernandez-Ferreiros and M. Angeles Gomez-Molleda, *Deciding the nilpotency of the Galois group by computing elements in the centre*, Math. Comp. **73** (2004), no. 248, 2043–2060 (electronic). MR MR2059750 (2005c:12005)

[13] Louis Granboulan, *Construction d'une extension régulière de* $\mathbf{Q}(T)$ *de groupe de Galois* M_{24}, Experiment. Math. **5** (1996), no. 1, 3–14. MR MR1412950 (98c:12006)

[14] Farshid Hajir, *On the Galois group of generalized Laguerre polynomials*, J. Théor. Nombres Bordeaux **17** (2005), no. 2, 517–525. MR MR2211305 (2006k:11218)

[15] ———, *Tame pro-p Galois groups: A survey of recent work*, Arithmetic, Geometry and Coding Theory (AGCT 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris, 2005, pp. 111–124. MR MR2182839

[16] Emmanuel Hallouin, *Study and computation of a Hurwitz space and totally real* $\mathrm{PSL}_2(F_8)$*-extensions of* Q, J. Algebra **292** (2005), no. 1, 259–281. MR MR2166804 (2006h:14041)

[17] G. Hanrot and F. Morain, *Solvability by radicals from an algorithmic point of view*, Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2001, pp. 175–182 (electronic). MR MR2049746 (2005a:11200)

[18] Florent Jouve, Emmanuel Kowalski, and David Zywina, *An explicit integral polynomial whose splitting field has galois group* $W(E_8)$, J. Théor. Nombres Bordeaux **20** (2008), no. 3, 761–782. MR MR2523316

[19] Gregor Kemper and Gunter Malle, *Invariant fields of finite irreducible reflection groups*, Math. Ann. **315** (1999), no. 4, 569–586. MR MR1731462 (2001c:13006)

[20] Masanari Kida, Guénaël Renault, and Kazuhiro Yokoyama, *Quintic polynomials of Hashimoto-Tsunogai, Brumer and Kummer*, Int. J. Number Theory **5** (2009), no. 4, 555–571. MR MR2532276

[21] Jürgen Klüners and Gunter Malle, *Explicit Galois realization of transitive groups of degree up to 15*, J. Symbolic Comput. **30** (2000), no. 6, 675–716, Algorithmic methods in Galois theory. MR MR1800033 (2001i:12005)

[22] Aristides Kontogeorgis, *The group of automorphisms of cyclic extensions of rational function fields*, J. Algebra **216** (1999), no. 2, 665–706. MR MR1692965 (2000f:12005)

[23] Jörn Müller-Quade and Rainer Steinwandt, *Recognizing simple subextensions of purely transcendental field extensions*, Appl. Algebra Engrg. Comm. Comput. **11** (2000), no. 1, 35–41. MR MR1817697 (2002g:12004)

[24] Renault Guénaél Renault, *Computation of the splitting field of a dihedral polynomial*, ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM Press, 2006, pp. 290–297.

[25] Núria Vila Sara Arias-de Reyna, *Tame Galois realizations of $GSp_4(F_l)$ over Q*, 2009.

[26] Romyar T. Sharifi, *On Galois groups of unramified pro-p extensions*, Math. Ann. **342** (2008), no. 2, 297–308. MR MR2425144

[27] Blair K. Spearman, Kenneth S. Williams, and Qiduan Yang, *The 2-power degree subfields of the splitting fields of polynomials with Frobenius Galois groups*, Comm. Algebra **31** (2003), no. 10, 4745–4763. MR MR1998026 (2004f:12001)

[28] Rainer Steinwandt and Jörn Müller-Quade, *Freeness, linear disjointness, and implicitization—a classical approach*, Beiträge Algebra Geom. **41** (2000), no. 1, 57–66. MR MR1745579 (2001a:12011)

Semifields and Near-fields

12Kxx

[1] Simeon Ball, Gary Ebert, and Michel Lavrauw, *A geometric construction of finite semifields*, J. Algebra **311** (2007), no. 1, 117–129. MR MR2309880

[2] Robert S. Coulter and Marie Henderson, *Commutative presemifields and semifields*, Adv. Math. **217** (2008), no. 1, 282–304. MR MR2365198

[3] Robert S. Coulter, Marie Henderson, and Pamela Kosick, *Planar polynomials for commutative semifields with specified nuclei*, Des. Codes Cryptogr. **44** (2007), no. 1-3, 275–286. MR MR2336411

[4] G. L. Ebert, O. Polverino, G. Marino, and R. Trombetti, *Semifields in class* $F_4^{(a)}$, Electron. J. Combin. **16** (2009), no. 1, 20. MR MR2505095

[5] Gary L. Ebert, Giuseppe Marino, Olga Polverino, and Rocco Trombetti, *On the multiplication of some semifields of order* q^6, Finite Fields Appl. **15** (2009), no. 2, 160–173. MR MR2494332

[6] Jill Hanson and Michael J. Kallaher, *Finite Bol quasifields are nearfields*, Utilitas Math. **37** (1990), 45–64. MR MR1068509 (92b:51024)

[7] K. J. Horadam and D. G. Farmer, *Bundles, presemifields and nonlinear functions*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 79–94. MR MR2438442

[8] Norman L. Johnson, Giuseppe Marino, Olga Polverino, and Rocco Trombetti, *On a generalization of cyclic semifields*, J. Algebraic Combin. **29** (2009), no. 1, 1–34. MR MR2470113 (2010e:12010)

[9] Giuseppe Marino and Rocco Trombetti, *A new semifield of order* 2^{10}, Discrete Math. **310** (2010), no. 22, 3108–3113.

[10] I. F. Rúa, Elías F. Combarro, and J. Ranilla, *Classification of semifields of order 64*, J. Algebra **322** (2009), no. 11, 4011–4029. MR MR2556135

Computational Methods

12-04

[1] Gregory V. Bard, Nicolas T. Courtois, and Chris Jefferson, *Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over* GF(2) *via SAT-solvers*, 2007.

[2] Cristina Bertone, Guillaume Chéze, and André Galligo, *Modular Las Vegas algorithms for polynomial absolute factorization*, J. Symbolic Comput. **45** (2010), no. 12, 1280–1295.

[3] Thomas Beth, Jörn Müller-Quade, and Rainer Steinwandt, *Computing restrictions of ideals in finitely generated k-algebras by means of Buchberger's algorithm*, J. Symbolic Comput. **41** (2006), no. 3-4, 372–380. MR MR2202557 (2006j:13027)

[4] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt, *Complexity issues in bivariate polynomial factorization*, ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM Press, 2004, pp. 42–49.

[5] Guillaume Chèze and Grégoire Lecerf, *Lifting and recombination techniques for absolute factorization*, J. Complexity **23** (2007), no. 3, 380–420. MR MR2330992

[6] Akpodigha Filatei, Xin Li, Marc Moreno Maza, and Éric Schost, *Implementation techniques for fast polynomial arithmetic in a high-level programming environment*, ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM Press, 2006, pp. 93–100.

[7] Katharina Geißler and Jürgen Klüners, *Galois group computation for rational polynomials*, J. Symbolic Comput. **30** (2000), no. 6, 653–674, Algorithmic methods in Galois theory. MR MR1800032 (2001k:12006)

[8] Kiran S. Kedlaya, *Search techniques for root-unitary polynomials*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 71–81. MR MR2459990 (2009h:26022)

[9] Sara Khodadad and Michael Monagan, *Fast rational function reconstruction*, ISSAC 2006, ACM, New York, 2006, pp. 184–190. MR MR2289118

[10] Grégoire Lecerf, *New recombination algorithms for bivariate polynomial factorization based on Hensel lifting*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 2, 151–176. MR 2600710

[11] Hsin-Chao Liao and Richard J. Fateman, *Evaluation of the heuristic polynomial GCD*, ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM Press, 1995, pp. 240–247.

[12] Michael Monagan, *Maximal quotient rational reconstruction: An almost optimal algorithm for rational reconstruction*, ISSAC 2004, ACM, New York, 2004, pp. 243–249. MR MR2126950 (2005j:68137)

[13] Jörn Müller-Quade and Rainer Steinwandt, *Basic algorithms for rational function fields*, J. Symbolic Comput. **27** (1999), no. 2, 143–170. MR MR1672124 (2000a:13043)

[14] ———, *Gröbner bases applied to finitely generated field extensions*, J. Symbolic Comput. **30** (2000), no. 4, 469–490. MR MR1784753 (2001i:13040)

[15] Fatima K. Abu Salem and Rawan N. Soudah, *An empirical study of cache-oblivious polygon indecomposability testing*, Computing **88** (2010), no. 8, 55–78.

[16] Leonard Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), no. 3, 273–281. MR MR797178 (87a:12002)

[17] Allan Steel, *A new scheme for computing with algebraically closed fields*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 491–505. MR MR2041106 (2005b:12016)

[18] Allan K. Steel, *Computing with algebraically closed fields*, J. Symbolic Comput. **45** (2010), no. 3, 342–372.

[19] Rainer Steinwandt, *On computing a separating transcendence basis*, SIGSAM Bulletin **34** (2000), no. 4.