

Field Theory

Field Theory: General

12E_{xx}

- [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(1):158–168, 2001.
- [2] B. V. Petrenko. On the product of two primitive elements of maximal subfields of a finite field. *J. Pure Appl. Algebra*, 178(3):297–306, 2003.
- [3] B. V. Petrenko. On the sum of two primitive elements of maximal subfields of a finite field. *Finite Fields Appl.*, 9(1):102–116, 2003.
- [4] Ruth Schwingel. The tensor product of polynomials. *Experiment. Math.*, 8(4):395–397, 1999.
- [5] Kirby C. Smith and Leon van Wyk. A concrete matrix field description of some Galois fields. *Linear Algebra Appl.*, 403:159–164, 2005.

Field Theory

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(2):608–635, 2001.
- [2] Bill Allombert. An efficient algorithm for the computation of Galois automorphisms. *Math. Comp.*, 73(245):359–375 (electronic), 2004.
- [3] Johan Bosman. A polynomial with Galois group $SL_2(F_{16})$. *LMS J. Comput. Math.*, 10:1461–1570 (electronic), 2007.
- [4] Nigel Boston. Reducing the Fontaine-Mazur conjecture to group theory. In *Progress in Galois theory*, volume 12 of *Dev. Math.*, pages 39–50. Springer, New York, 2005.
- [5] Nigel Boston and Charles Leedham-Green. Explicit computation of Galois p -groups unramified at p . *J. Algebra*, 256(2):402–413, 2002.
- [6] Nigel Boston and Harris Nover. Computing pro- p -Galois groups. In *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 1–10. Springer, Berlin, 2006.
- [7] Nigel Boston and David Perry. Maximal 2-extensions with restricted ramification. *J. Algebra*, 232(2):664–672, 2000.
- [8] Antoine Colin. Relative resolvents and partition tables in Galois group computations. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 78–84 (electronic), New York, 1997. ACM.
- [9] Lassina Dembélé. A non-solvable galois extension of q ramified at 2 only. *C. R., Math., Acad. Sci. Paris*, 347(3-4), 2009.
- [10] Michael Dettweiler. Galois realizations of classical groups and the middle convolution. [arXiv:math.NT/0605381v1](https://arxiv.org/abs/math.NT/0605381v1), 94 pages, 2006.

- [11] Pilar Fernandez-Ferreiros and M. Angeles Gomez-Molleda. Deciding the nilpotency of the Galois group by computing elements in the centre. *Math. Comp.*, 73(248):2043–2060 (electronic), 2004.
- [12] Louis Granboulan. Construction d’une extension régulière de $\mathbf{Q}(T)$ de groupe de Galois M_{24} . *Experiment. Math.*, 5(1):3–14, 1996.
- [13] Farshid Hajir. On the Galois group of generalized Laguerre polynomials. *J. Théor. Nombres Bordeaux*, 17(2):517–525, 2005.
- [14] Farshid Hajir. Tame pro- p Galois groups: A survey of recent work. In *Arithmetic, Geometry and Coding Theory (AGCT 2003)*, volume 11 of *Sémin. Congr.*, pages 111–124. Soc. Math. France, Paris, 2005.
- [15] Emmanuel Hallouin. Study and computation of a Hurwitz space and totally real $\mathrm{PSL}_2(F_8)$ -extensions of Q . *J. Algebra*, 292(1):259–281, 2005.
- [16] G. Hanrot and F. Morain. Solvability by radicals from an algorithmic point of view. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 175–182 (electronic), New York, 2001. ACM.
- [17] 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(3):761–782, 2008.
- [18] Gregor Kemper and Gunter Malle. Invariant fields of finite irreducible reflection groups. *Math. Ann.*, 315(4):569–586, 1999.
- [19] Jürgen Klüners and Gunter Malle. Explicit Galois realization of transitive groups of degree up to 15. *J. Symbolic Comput.*, 30(6):675–716, 2000.
- [20] Aristides Kontogeorgis. The group of automorphisms of cyclic extensions of rational function fields. *J. Algebra*, 216(2):665–706, 1999.
- [21] Jörn Müller-Quade and Rainer Steinwandt. Recognizing simple subextensions of purely transcendental field extensions. *Appl. Algebra Engrg. Comm. Comput.*, 11(1):35–41, 2000.

- [22] Guénael Renault. Computation of the splitting field of a dihedral polynomial. In *ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation*, pages 290–297, New York, NY, USA, 2006. ACM Press.
- [23] Romyar T. Sharifi. On Galois groups of unramified pro- p extensions. *Math. Ann.*, 342(2):297–308, 2008.
- [24] 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(10):4745–4763, 2003.
- [25] Rainer Steinwandt and Jörn Müller-Quade. Freeness, linear disjointness, and implicitization—a classical approach. *Beiträge Algebra Geom.*, 41(1):57–66, 2000.

Field Theory

Semifields and Near-fields

12Kxx

- [1] Simeon Ball, Gary Ebert, and Michel Lavrauw. A geometric construction of finite semifields. *J. Algebra*, 311(1):117–129, 2007.
- [2] Robert S. Coulter and Marie Henderson. Commutative presemifields and semifields. *Adv. Math.*, 217(1):282–304, 2008.
- [3] Robert S. Coulter, Marie Henderson, and Pamela Kosick. Planar polynomials for commutative semifields with specified nuclei. *Des. Codes Cryptogr.*, 44(1-3):275–286, 2007.
- [4] G. L. Ebert, O. Polverino, G. Marino, and R. Trombetti. Semifields in class $F_4^{(a)}$. *Electron. J. Combin.*, 16(1):20, 2009.
- [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(2):160–173, 2009.
- [6] K. J. Horadam and D. G. Farmer. Bundles, presemifields and nonlinear functions. *Des. Codes Cryptogr.*, 49(1-3):79–94, 2008.
- [7] Norman L. Johnson, Giuseppe Marino, Olga Polverino, and Rocco Trombetti. On a generalization of cyclic semifields. *J. Algebraic Combin.*, 29(1):1–34, 2009.
- [8] Giuseppe Marino and Rocco Trombetti. A new semifield of order 2^{10} . *Discrete Math.*, In Press, 2009.
- [9] I.F. Rua, Elias F. Combarro, and J. Ranilla. Classification of semifields of order 64. *J. Algebra*, In Press, 2009.

Field Theory

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 $\text{GF}(2)$ via SAT-solvers. *IACR eprint:2007:024*, 14 pages, 2007.
- [2] 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(3-4):372–380, 2006.
- [3] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt. Complexity issues in bivariate polynomial factorization. In *ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, pages 42–49, New York, NY, USA, 2004. ACM Press.
- [4] Guillaume Chèze and Grégoire Lecerf. Lifting and recombination techniques for absolute factorization. *J. Complexity*, 23(3):380–420, 2007.
- [5] Akpodigha Filatei, Xin Li, Marc Moreno Maza, and Éric Schost. Implementation techniques for fast polynomial arithmetic in a high-level programming environment. In *ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation*, pages 93–100, New York, NY, USA, 2006. ACM Press.
- [6] Katharina Geissler and Jürgen Klüners. Galois group computation for rational polynomials. *J. Symbolic Comput.*, 30(6):653–674, 2000.
- [7] Kiran S. Kedlaya. Search techniques for root-unitary polynomials. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 71–81. Amer. Math. Soc., Providence, RI, 2008.
- [8] Sara Khodadad and Michael Monagan. Fast rational function reconstruction. In *ISSAC 2006*, pages 184–190. ACM, New York, 2006.

- [9] Hsin-Chao Liao and Richard J. Fateman. Evaluation of the heuristic polynomial GCD. In *ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation*, pages 240–247, New York, NY, USA, 1995. ACM Press.
- [10] Michael Monagan. Maximal quotient rational reconstruction: An almost optimal algorithm for rational reconstruction. In *ISSAC 2004*, pages 243–249. ACM, New York, 2004.
- [11] Jörn Müller-Quade and Rainer Steinwandt. Basic algorithms for rational function fields. *J. Symbolic Comput.*, 27(2):143–170, 1999.
- [12] Jörn Müller-Quade and Rainer Steinwandt. Gröbner bases applied to finitely generated field extensions. *J. Symbolic Comput.*, 30(4):469–490, 2000.
- [13] Leonard Soicher and John McKay. Computing Galois groups over the rationals. *J. Number Theory*, 20(3):273–281, 1985.
- [14] Allan Steel. A new scheme for computing with algebraically closed fields. In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 491–505. Springer, Berlin, 2002.
- [15] Allan K. Steel. Computing with algebraically closed fields. *J. Symbolic Comput.*, To appear, 2009.
- [16] Rainer Steinwandt. On computing a separating transcendence basis. *SIGSAM Bulletin*, 34(4), 2000.