Fried, Michael D.; **Guralnick, Robert**; **Saxl, Jan**
Schur covers and Carlitz's conjecture. (English) Zbl 0855.11063
Isr. J. Math. 82, No. 1-3, 157-225 (1993).

In this seminal paper the authors prove the Carlitz conjecture from 1966 which says that if q is an odd prime power, then any exceptional polynomial over the finite field F_q must have odd degree. Recall that a polynomial over F_q is called exceptional if it is a permutation polynomial of infinitely many finite extensions of F_q. For the historical background on the Carlitz conjecture and equivalent formulations [see *R. Lidl* and *G. L. Mullen*, Am. Math. Mon. 95, 243-246 (1988; Zbl 0653.12010), ibid. 100, 71-74 (1993; Zbl 0777.11054)].

The starting point of the proof of the conjecture is what the authors call the exceptionality lemma, which gives a characterization of exceptional polynomials in terms of their geometric-arithmetic monodromy group pair. Both monodromy groups naturally come with permutation representations, and this establishes an important link with the theory of permutation groups. Another crucial ingredient of the proof is the ramification theory of covers of curves in positive characteristic.

The paper contains a wealth of additional information on exceptional polynomials. For example, it is shown that if F_q has characteristic $p > 3$, then any exceptional polynomial over F_q is a composition of cyclic polynomials, Chebyshev polynomials, and polynomials of degree a power of p. This is a consequence of the result that for $p > 3$ the arithmetic monodromy group of an indecomposable exceptional polynomial is an affine group, and the proof of this result relies in turn on the classification of finite simple groups.

Reviewer: H.Niederreiter (Wien)

MSC:

11T06	Polynomials over finite fields
14H30	Coverings of curves, fundamental group
20D30	Series and lattices of subgroups
12E10	Special polynomials in general fields

Keywords:

Schur covers; Carlitz conjecture; exceptional polynomial; permutation polynomial; monodromy groups; permutation representations; permutation groups; covers of curves; cyclic polynomials; Chebyshev polynomials

Full Text: DOI

References:

[1] S. Abhyankar,Coverings of Algebraic Curves, Am. J. Math79 (1957), 825–856. · Zbl 0087.03603 · doi:10.2307/2372438

[2] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson,Atlas of finite groups: maximal subgroups and ordinary characters for simple groups, Clarendon Press, New York, 1985. · Zbl 0568.20001

[3] M. Aschbacher,On the maximal subgroups of the finite classical groups, Invent. Math.76 (1984), 469–514. · Zbl 0537.20023 · doi:10.1007/BF01388470

[4] M. Aschbacher and L. Scott,Maximal subgroups of finite groups, J. Algebra92 (1985), 44–80. · Zbl 0549.20011 · doi:10.1016/0021-8693(85)90145-0

[5] A. Borel and J. Tits,Elements unipotents et sous-groupes paraboliques de groupes reductif I, Invent. Math.12 (1971), 95–104. · Zbl 0238.20055 · doi:10.1007/BF01404653

[6] W. Burnside,On simply transitive groups of prime degree, Quart. J. Math.37 (1906), 215–236. · Zbl 37.0172.01

[7] P. Cameron,Finite permutation groups and finite simple groups, BLMS13 (1981), 1–22. · Zbl 0463.20003

[8] R. Carter,Simple Groups of Lie Type, John Wiley \& Sons, New York, 1989. · Zbl 0723.20006

[9] S. Cohen,Permutation Polynomials and Primitive Permutation Groups, Arch. Math.57 (1991), 417–423. · Zbl 0766.11047 · doi:10.1007/BF01246737

[10] S. Cohen,Exceptional polynomials and the reducibility of substitution polynomials,, L'Enseigment Math.36 (1990), 309–318.

· Zbl 0728.11065

[11] J. W. S. Cassels and J. Fröhlich,Algebraic Number Theory, Acad. Press, London and New York, 1967.

[12] H. Davenport and D. J. Lewis,Notes on Congruences (I), Quart. J. Math14 (1963), 51–60. · Zbl 0113.26704 · doi:10.1093/qmath/14.1.51

[13] L. E. Dickson,The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Ann. of Math.11 (1897), 65–120, 161–183. · Zbl 28.0135.03 · doi:10.2307/1967217

[14] M. Fried,Exposition on an Arithmetic-Group Theoretic Connection via Riemann's Existence Theorem, Proceedings of Symposia in Pure Math: Santa Cruz Conference on Finite Groups, A.M.S. Publications37 (1980), 571–601. · Zbl 0451.14011

[15] M. Fried,Arithmetical properties of function fields (II); the generalized Schur problem, Acta Arith.XXV (1974), 225–258. · Zbl 0229.12020

[16] M. Fried,On a conjecture of Schur, Mich. Math. Journal17 (1970), 41–55. · Zbl 0169.37702 · doi:10.1307/mmj/1029000374

[17] M. Fried,On a theorem of MacCluer, Acta Arith.XXV (1974), 122–127. · Zbl 0229.12021

[18] M. Fried,Galois groups and complex multiplication, Trans.A.M.S.235 (1978), 141–162. · Zbl 0394.14010 · doi:10.1090/S0002-9947-1978-0472917-6

[19] M. Fried,The Nonregular Analogue of Tchebotarev's Theorem, Pac. Journ.113 (1984), 1–9. · Zbl 0551.12009

[20] M. Fried and M. Jarden,Field Arithmetic, Springer Ergebnisse series, Vol 11, 1986.

[21] A. Grothendieck,Géométrie formelle et géométrie algébrique, Seminaire Bourbaki t. 11182 (1958/59).

[22] R. Guralnick,Subgroups of prime power index in a simple group, J. Algebra81 (1983), 304–311. · Zbl 0515.20011 · doi:10.1016/0021-8693(83)90190-4

[23] D. Hayes,A geometric approach to permutation polynomials over a finite field, Duke Math. J.34 (1967), 293–305. · Zbl 0163.05202 · doi:10.1215/S0012-7094-67-03433-3

[24] D. Harbater,Formal Patching and Adding Branch Points, preprint June 1991. · Zbl 0790.14027

[25] C. Hering, M. W. Liebeck and J. Saxl,The factorizations of the finite exceptional groups of Lie Type, J. Alg.106 (1987), 517–527. · Zbl 0607.20012 · doi:10.1016/0021-8693(87)90013-5

[26] B. Huppert,Endliche Gruppen I, Springer, New York-Heidelberg-Berlin, 1967. · Zbl 0217.07201

[27] P. Kleidman and M. W. Liebeck,The subgroup structure of the finite classical groups, LMS Lecture Notes \#129, Cambridge University Press, Cambridge, (1990). · Zbl 0697.20004

[28] R. Lidl and G. Mullen,When does a polynomial over a finite field permute the elements of a field, II, Amer. Math Monthly100 \#1 (1993), 71–74. · Zbl 0777.11054

[29] R. Lidl and H. Niederreiter,Finite Fields, Encyclo. Math. and Appls., Addison-Wesley, Reading MA.20 (1983), now distributed by Cambridge University Press. · Zbl 0554.12010

[30] M. W. Liebeck,On the orders of the maximal subgroups of the finite classical groups, Proc. London Math. Soc.50 (1985), 426–446. · Zbl 0591.20021 · doi:10.1112/plms/s3-50.3.426

[31] M. Liebeck, C. Praeger, J. Saxl,The maximal factorizations of the finite simple groups and their automorphism groups, Mem. AMS86 \#432 (1990). · Zbl 0703.20021

[32] M. Liebeck, C. Praeger and J. Saxl,On the 2-closures of finite permutation groups, J. London Math. Soc.37 (1988), 241–252. · Zbl 0655.20003 · doi:10.1112/jlms/s2-37.2.241

[33] M. Liebeck, C. Praeger, J. Saxl,On the O'Nan-Scott reduction theorem for finite primitive permutation groups, J. Australian Math. Soc. A44 (1988), 389–396 (MR: 89a:20002). · Zbl 0647.20005 · doi:10.1017/S144678870003216X

[34] M.W. Liebeck and J. Saxl,The primitive permutation groups of odd degree, J. London Math. Soc.31 (1985), 250–264. · Zbl 0573.20004 · doi:10.1112/jlms/s2-31.2.250

[35] P. Mueller,A degree 21 counterexample to the Indecomposability Statement, e-mail February 8, 1993.

[36] G.L. Mullen,Permutation polynomials over finite fields, Proc. Inter. Conf. Finite Fields, Coding Theory and Appls. in Comm. and Comp., Las Vegas, NV, Aug. 1991, Lecture Notes in Pure and Appl. Math., Marcel Dekker (1992), pp. 131–151.

[37] M. Raynaud,Revêtements de la droite affine en caractéristique p>0et conjecture d'Abhyankar, preprint, to appear in Inventiones.

[38] A. Schinzel,Selected Topics on Polynomials, Ann Arbor, The University of Michigan Press, 1982.

[39] I. Schur,Über den Zussamenhang zwischen einem Problem der Zahlentheorie und linier satz über algebraische Functionen, S.-B. Preuss. Akad. Wiss. Phys.-Math. K. (1923), pp. 123–134. · Zbl 49.0093.02

[40] I. Schur,Zur Theorie der einfach transitiven Permutations Gruppen, S.-B. Preuss. Akad. Wiss. Phys.-Math. Kl. (1933), pp. 598–623. · Zbl 0007.14903

[41] G. Seitz,Unipotent subgroups of groups of Lie type, J. Algebra84 (1983), 253–278. · Zbl 0527.20031 · doi:10.1016/0021-8693(83)90078-9

[42] J.-P. Serre,Construction de revêtement étales de la droite affine de caractéristic p, Comptes Rendus311 (1990), 341–346.

[43] J.-P. Serre,Revêtements de courbes algébriques, Sém. Bour., 44ème année n{\(\deg\)}749 (1991/92).

[44] J.-P. Serre,Topics in Galois Theory, Research Notes in Mathematics, Jones and Bartlett, 1992. · Zbl 0746.12001

[45] D. Wan,Permutation polynomials and resolution of singularities over finite fields, Proc. Amer. Math. Soc.110 (1990), 303–309. · Zbl 0711.11050 · doi:10.1090/S0002-9939-1990-1031673-4

[46] H. Wielandt, Primitive Permutationsgruppen von Grad 2p, Math. Z.63 (1956), 478–485. · Zbl 0071.02303 · doi:10.1007/BF01187953