

PERMUTATION POLYNOMIALS IN ONE
AND SEVERAL VARIABLES

REX W. MATTHEWS

Various authors have dealt with problems relating to permutation polynomials over finite systems (see references). In this thesis various known results are extended and several questions are resolved.

Chapter 2 begins by considering the problem of finding those permutation polynomials in a single variable amongst some given classes of polynomials. Previously, this question was settled only for cyclic polynomials and Chebyshev polynomials of the first kind. Here we consider the Chebyshev polynomials of the second kind and polynomials of the form $(x^n - 1)/(x - 1)$. Certain questions on multivariable polynomials are then considered.

Chapter 3 deals with questions involving polynomials whose coefficients lie in a subfield of the given field, and considers some combinatorial questions.

Chapter 4 resolves the structure of the group of maps of $\mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ induced by the extended Chebyshev polynomials of Lidl and Wells [9].

Chapter 5 extends this further to finite rings $\mathbb{Z}/(p^e)$, thus generalising results of Lausch, Müller and Nöbauer [4].

Chapter 6 settles some questions concerning the conjecture of Schur on polynomials $f(x) \in \mathbb{Z}[x]$ which permute infinitely many residue fields

Received 20 July 1983. Thesis submitted to University of Tasmania, October 1982. Degree approved May 1983. Supervisor: Professor R. Lidl.

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9727/83
\$A2.00 + 0.00.

\mathbb{F}_p . It is known [3] that these are compositions of cyclic and Chebyshev polynomials of the first kind. In Chapter 6 it is determined which of these polynomials have the required property.

References

- [1] L. Carlitz and J. Hayes, "Permutations with coefficients in a subfield", *Acta Arith.* 21 (1972), 131-135.
- [2] L.E. Dickson, *Linear groups* (Dover, New York, 1958).
- [3] M. Fried, "On a conjecture of Schur", *Michigan Math. J.* 17 (1970), 41-55.
- [4] H. Lausch, W. Müller und W. Nöbauer, "Über die Struktur einer durch Dicksonpolynome dargestellten Permutationsgruppe des Restklassenringes modulo n ", *J. Reine Angew. Math.* 261 (1973), 88-99.
- [5] R. Lidl, "Tschebyscheffpolynome und die dadurch dargestellten Gruppen", *Monatsh. Math.* 77 (1973), 132-147.
- [6] R. Lidl, "Über die Struktur einer durch Tschebyscheffpolynome in 2 Variablen dargestellten Permutationsgruppe", *Beiträge Algebra Geom.* 3 (1974), 41-48.
- [7] R. Lidl, "Tschebyscheffpolynome in mehreren Variablen", *J. Reine Angew. Math.* 273 (1975), 178-198.
- [8] R. Lidl and H. Niederreiter, "On orthogonal systems and permutation polynomials in several variables", *Acta Arith.* 22 (1973), 257-265.
- [9] R. Lidl and C. Wells, "Chebyshev polynomials in several variables", *J. Reine Angew. Math.* 255 (1972), 104-111.
- [10] R. Matthews, "Orthogonal systems of polynomials over a finite field with coefficients in a subfield", *Contemporary mathematics*, 9, 295-302 (American Mathematical Society, Providence, Rhode Island, 1982).

- [11] R. Matthews, "Some generalisations of Chebyshev polynomials and their induced group structure over a finite field", *Acta Arith.* **41** (1982), 323-335.
- [12] R. Matthews, "The structure of the group of permutations induced by Chebyshev polynomial vectors over the ring of integers mod m ", *J. Austral. Math. Soc. Ser. A* **32** (1982), 88-103.
- [13] R. Matthews, "Permutation polynomials over rings of algebraic integers", *J. Number Theory* (to appear).
- [14] H. Niederreiter, "Orthogonal systems of polynomials in finite fields", *Proc. Amer. Math. Soc.* **28** (1971), 415-422.
- [15] H. Niederreiter and S. Lo, "Permutation polynomials over rings of algebraic integers", *Abh. Math. Sem. Univ. Hamburg* **49** (1979), 126-139.

Department of Mathematics,
University of Tasmania,
Hobart,
Tasmania 7001,
Australia.