PERMUTATION POLYNOMIALS IN ONE AND SEVERAL VARIABLES

by

illiam.

Rex W. Matthews, B.A., B.Sc.(Hons), Dip.Ed.

Submitted in fulfilment of the requirements for

the degree of

Doctor of Philosophy

University of Tasmania

Hobart

October, 1982

(conferral date unknown at present)

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Professor R. Lidl, for his advice and encouragement during the preparation of this thesis. I am also appreciative of the financial assistance provided by a University of Tasmania Postgraduate Award.

Finally, I would like to thank Mrs. C. Lowry for her excellent typing.

Except as stated herein, this thesis contains no material which has been accepted for the award of any other degree or diploma in any university, and to the best of my knowledge and belief, contains no copy or paraphrase of material previously published or written by another person except where duly acknowledged.

Rex W. Matthews.

Some of the results of this thesis have been published or are to be published under my sole authorship. A list of these publications follows.

1 Orthogonal systems of polynomials over a finite field with coefficients in a subfield, in Contemporary Mathematics ,vol. 9, 1982, pp. 295-302 (A.M.S.)

2.Some generalisations of Chebyshev polynomials and their induced group structure over a finite field, Acta Arithmetica, to appear

3.The structure of the group of permutations induced by Chebyshev polynomial vectors over the ring of integers mod m, J. Aust. Math. Soc., 32 (1982), pp. 88-103.

4.Permutation polynomials over rings of algebraic integers, J. Number Theory, to appear.

ABSTRACT

Various authors have dealt with problems relating to permutation polynomials over finite systems ([4], [8], [10], [18], [20]-[25],[29]-[33], etc.). 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 $\mathbb{F}_q^n \to \mathbb{F}_q^n$ induced by the extended Chebyshev polynomials of Lidl and Wells [26]. Chapter 5 extends this further to finite rings $\mathbb{Z}/(p^e)$, thus generalising results of Lausch-Müller-Nöbauer [18].

Chapter 6 settles some questions concerning the conjecture of Schur on polynomials $f(x) \in \mathbb{Z}[x]$ which permute infinitely many residue fields $\mathbb{F}_p$. It is known ([10]) 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.

CONTENTS

INTRODUCTION

This thesis deals with various properties of polynomials in one or several variables over a finite field or a finite ring.

Chapter 1 introduces finite fields and Galois rings, which are used in subsequent chapters. This is followed by a brief discussion of algebraic number theory, and some results on circulant matrices are noted.

Chapter 2 gives the fundamental concepts of a permutation polynomial and an orthogonal system.The cyclic and Dickson polynomials are defined and permutation properties of Chebyshev polynomials of the second kind are discussed.

Polynomials in several variables are then considered. The classical König-Rados theorem is given in a multivariable form, and a result of Horakova and Schwarz [16] is generalised to yield information on the distribution of the zeros of a multivariable polynomial by degree. Circulant matrices are used to obtain a criterion for a multivariable polynomial to be a permutation polynomial. A detailed discussion of sums of polynomials in several variables is presented in theorem 2.8. This question was previously settled only in the prime field case. Similarly, theorem 2.9 extends a criterion of Niederreiter [31] from the prime case.

We then consider κ-polynomials, which distribute their values uniformly over $\mathbb{F}_q^*$. The question is considered of deciding when a product of polynomials in disjoint sets of variables is a κ-polynomial, in analogy with the corresponding sums of permutation polynomials. The criteria turn out, however, to be quite different. Thus, over $\mathbb{F}_p$, f + g is a permutation polynomial if and only if either f or g is one, but fg may be a κ-polynomial even though neither f nor g is. A character sum criterion for κ-polynomials is given.

Finally, permutation properties of the elementary symmetric functions over $\mathbb{F}_q$ are considered. Certain of these are shown to be permutation polynomials. These have the property that they remain permutation polynomials over all extension fields of $\mathbb{F}_p$. Other polynomials with this property are also presented.

Niederreiter [30] has shown that any orthogonal system $(f_1,\ldots,f_r)$ in n variables, $r < n$, may be completed to an orthogonal system $(f_1,\ldots,f_n)$. Carlitz and Hayes [4], considered the question of elucidating the structure of the group of permutations of $\mathbb{F}_{q^t}$ induced by single-variable polynomials which actually belong to $\mathbb{F}_q[x]$. We extend this result to orthogonal systems in chapter 3, then consider Niederreiter's extension problem, where $(f_1,\ldots,f_r)$ is an orthogonal system over $\mathbb{F}_{q^t}$, with $f_i \in \mathbb{F}_q[x_1,\ldots,x_n]$, and ask whether this may be extended to $(f_1,\ldots,f_n)$, with $f_i \in \mathbb{F}_q[x_1,\ldots,x_n]$ and $(f_1,\ldots,f_n)$ an orthogonal system over $\mathbb{F}_{q^t}$. Such extensions are enumerated in this chapter.

In the last three chapters we deal with properties of cyclic and Chebyshev polynomials. Chapters 4 and 5 deal with the multivariable Chebyshev polynomials introduced by Lidl and Wells [26]. Chapter 4 begins by placing these in a more general setting, where we derive a multivariable polynomial vector from a single-variable polynomial. We then relate the properties of these two objects, the key result being theorem 4.1. The structure of all permutations obtained in this way is obtained, then the group of maps induced by the generalised Chebyshev polynomials over $\mathbb{F}_q$ is determined. This extends results of Lidl ([20] and [21]) from the two-variable case. We conclude chapter 4 with a short proof of a result of Brawley, Carlitz and Levine [3] on matrix permutation polynomials, which uses the construction of this chapter.

Chapter 5 extends the results of chapter 4 from finite fields to the ring of integers mod m. These results were known previously only for one variable ([18]). The chapter begins with an evaluation of the Jacobians of the polynomials defined in chapter 4, and the generalised Chebyshev polynomials. Regular polynomial vectors are discussed, and a regularity criterion for multivariable Chebyshev polynomials is given. The determination of the structure of the permutation group induced on $(\mathbb{Z}/(p^e))^n$ by the Chebyshev polynomials makes use of Galois rings and results of Ward [44] and [45] on linear recurring sequences.

In chapter 6 we consider a property of the single-variable cyclic and Chebyshev polynomials. Namely that these are permutation polynomials over infinitely many prime fields $\mathbb{F}_p$. Schur conjectured that they are essentially the only such polynomials, and Fried [10] proved this for residue class fields of an algebraic number field. This chapter completes the converse problem of deciding which cyclic or Chebyshev polynomials have this property for a given algebraic number field K. Previously [32] only the quadratic and cyclotomic fields had been settled, and a few general results were also known.

CHAPTER 1

BASIC RESULTS

In this chapter we introduce various results needed in later chapters and define some basic concepts. Proofs are omitted if references to the literature are available.

1. FINITE FIELDS AND GALOIS RINGS

For each prime $p \in \mathbb{Z}$, and prime power $q(= p^e)$ there exists, up to isomorphism, a unique finite field of order q, denoted $\mathbb{F}_q$. The following properties of $\mathbb{F}_q$ are well-known.

1. The multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is cyclic. A generator of $\mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q$.

2. $\mathbb{F}_q$ is the unique algebraic extension of $\mathbb{F}_p$ ($\simeq \mathbb{Z}/(p)$) of degree e.

If the ring $\mathbb{Z}/(p^n)$ is denoted by R, then one may seek extension rings of R which relate to R as $\mathbb{F}_q$ does to $\mathbb{F}_p$. Such rings are the Galois rings. They are considered in chapter XVI of McDonald [27]. Let μ denote the canonical homomorphism $\mu\colon \mathbb{Z}/(p^n) \to \mathbb{Z}/(p)$. Then $f(x) \in \mathbb{Z}/(p^n)[x]$ is called a basic irreducible if $\mu f(x)$ is irreducible over $\mathbb{Z}/(p)$. If this is the case then $f(x)$ is irreducible in $\mathbb{Z}/(p^n)$. If $f(x)$ is any basic irreducible of degree r, then all rings of the type $\mathbb{Z}/(p^n)[x]/(f)$ are isomorphic, and are called Galois rings, denoted $GR(p^n,r)$. Further, $GR(p^n,r) \simeq \mathbb{Z}[x]/(p^n,f)$, if $f(x) \in \mathbb{Z}[x]$, and f is irreducible mod p. There is a natural projection $\theta\colon GR(p^n,r) \to GR(p^{n-1},r)$ with kernel (p^{n-1}). Also, $GR(p^n,1) \simeq \mathbb{Z}/(p^n)$, and $GR(p,r) \simeq \mathbb{F}_{p^r}$. f splits uniquely into linear factors in $GR(p^n,r)$. We use the following results. Let $\mu\colon GR(p^n,r) \to \mathbb{F}_{p^r}$.

LEMMA 1.1. *(Hensel's lemma). Let* $h \in GR(p^n,r)[x]$ *and* $\mu h = \bar{g}_1 \cdots \bar{g}_t$, *where* $\bar{g}_1,\ldots,\bar{g}_t$ *are pair-wise coprime. Then there exist* $g_1,\ldots,g_t$, $g_i \in GR(p^n,r)[x]$ *such that*

(i) $g_1,\ldots,g_t$ *are pair-wise coprime;*

(ii) $\mu g_i = \bar{g}_i$, $1 \le i \le t$*;*

(iii) $h = g_1 \cdots g_t$.

PROOF. McDonald [27], page 256 proves this result for local rings. $GR(p^n,r)$ is a local ring.

If f is not a zero divisor in $GR(p^n,r)[x]$, then f is called regular.

LEMMA 1.2. *Let* $f \in GR(p^n,r)$ *be regular. Then*

(i) If μf *is irreducible in* $\mathbb{F}_{p^r}$*, then* f *is irreducible.*

(ii) If f *is irreducible then* $\mu f = \delta g^t$, *where* $\delta \in \mathbb{F}_{p^r}$, *and* g *is a monic irreducible in* $\mathbb{F}_{p^r}[x]$.

PROOF. McDonald [27], p. 260.

A local ring is a ring with exactly one maximal right (or left) ideal.

LEMMA 1.3. *Let* R *be a commutative local ring of characteristic* p^n *with maximal ideal* I *and residue field* k. *Let* $[k: \mathbb{Z}/(p)] = r$ *and* $\{u_1,\ldots,u_t\}$ *be a minimal* R*-generating set of* I. *Then there exists a subring* S *of* R *such that*

(i) $S \simeq GR(p^n,r)$ *where* S *is unique;*

(ii) R *is the ring homomorphic image of* $S[x_1,\ldots,x_t]$.

PROOF. McDonald [27], p. 337.

LEMMA 1.4. *Let* $T = GR(p^n, t)$, *and let* T^* *be the group of units of* T. *Then* $T^* = G_1 \times G_2$, *where*

(a) G_1 *is a cyclic group of order* $p^t - 1$;

(b) G_2 *is a group of order* $p^{(n-1)t}$, *such that*

(i) *if* p *is odd, or* $p = 2$ *and* $n \leq 2$, *then* G_2 *is a direct product of* t *cyclic groups of order* p^{n-1}.

(ii) *If* $p = 2$ *and* $n \geq 3$, *then* G_2 *is a direct product of a cyclic group of order* 2, *a cyclic group of order* 2^{n-2} *and* $t - 1$ *cyclic groups of order* 2^{n-1}.

PROOF. McDonald [27], p. 322.

2. NUMBER THEORETICAL RESULTS

We will need, particularly in chapter 6, some basic results from algebraic number theory. Here we establish some notation and describe the fundamental results on ideals in number fields. Hasse [15], Narkiewicz [28] and Weil [46] are standard works in this area.

Let K be a finite extension of $\mathbb{Q}$. Whereas classical number theory deals with properties of $\mathbb{Z}$, algebraic number theory deals with similar questions over a certain subring A of K. A is the ring of algebraic integers in K where $a \in K$ is an algebraic integer (over $\mathbb{Q}$) if it satisfies a monic equation with coefficients in $\mathbb{Z}$. The first major obstacle in extending number theoretical results to A is the lack of unique factorisation in A. This is restored by considering the ideals of A. The ideals of A have unique decomposition into products of powers of prime ideals. If P is a prime ideal of A, then $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, and so $P \cap \mathbb{Z} = p\mathbb{Z}$, for some prime $p \in \mathbb{Z}$. Further $pA = \prod_{i=1}^{t} P_i^{e_i}$, where P_i are prime ideals of A, and $P_i \cap \mathbb{Z} = p\mathbb{Z}$. The ideals P_i are said to lie over p. For all but finitely many primes $p \in \mathbb{Z}$, the powers e_i occurring in the decomposition of pA are unity. If this is not the case, then p is said to be ramified in A (or in K). If $t = 1$, and $e_1 = 1$, then p is said to remain inert in K. If $[K:\mathbb{Q}] = t$, then p is said to split completely in K. The integer e_i is called the ramification index of P_i over p, and f_i $(= [A/P_i; \mathbb{Z}/(p)]$ is called the inertia degree of P_i. If K is a normal extension of $\mathbb{Q}$ then the e_i's are equal, as are the f_i's. In any case $\sum e_i f_i = [K:\mathbb{Q}]$ and in the normal case, if $e_i = e$, $f_i = f$, then $tef = [K:\mathbb{Q}]$. Further $e_i | n$ and $f_i | n$. f is also written $f(P|p)$.

Now suppose K is a normal extension of $\mathbb{Q}$. Let P be a prime ideal of A lying over $p \in \mathbb{Z}$, with P unramified in K. Then corresponding to P there is a unique $\phi \in \mathrm{Gal}(K: \mathbb{Q})$ such that $\phi(\alpha) \equiv \alpha^p \bmod P$, for all $\alpha \in A$. ϕ is called the Frobenius automorphism of P. If K is abelian over $\mathbb{Q}$, ϕ depends only on p. The order of ϕ equals $f(P|p)$. Thus one obtains a map from the set of unramified prime ideals of A to $\mathrm{Gal}(K:\mathbb{Q})$ obtained by mapping an ideal to its Frobenius automorphism. This may be extended multiplicatively to the set of all unramified ideals of A. The resulting map is called the Artin map of A over $\mathbb{Q}$. The detailed properties of this map lead into class field theory. Finally we introduce some notation.

If I is an ideal of A, then the norm of I, $N_{K/\mathbb{Q}}(I)$ is defined to be $|A/I|$. This is always finite.

We will use the following result in chapter 5. The case $e = 1$ is well-known.

LEMMA 1.5. *There is a finite algebraic extension* K *of* $\mathbb{Q}$, *with ring of integers* A, *and a prime ideal* P *with* $P = pA$, *such that*

$$A/P^e \simeq GR(p^e,t) .$$

PROOF. Let f(x) be an irreducible monic polynomial of degree t over $\mathbb{Z}$ such that $\mu f(x)$ is irreducible over $\mathbb{Z}/(p)$. If α is a root of μf in $\mathbb{F}_{p^t}$, then $\mu f'(\alpha) \neq 0$. Thus disc $(\mu f) \neq 0$ in $\mathbb{Z}_p$, and so $p \nmid$ disc f over $\mathbb{Z}$. By the Kummer-Dedekind theorem on ideal factorisation (see [28] p. 161) p remains inert in $K = \mathbb{Q}[x]/(f(x))$. If A is the ring of integers of K, let $S = A/P^e$, where $P = pA$. Then char $S = p^e$, or else $p^{e-1} \in P^e$, and so $P^{e-1} \subseteq P^e$, a contradiction. Thus S is an extension ring of $\mathbb{Z}/(p^e)$. S is clearly a commutative local ring, $[A/P: \mathbb{Z}/(p)] = t$, and so S contains a subring $T \simeq GR(p^e,t)$, by lemma 1.3. Since $|S| = p^{et} = |T|$, $S = T$ completes the proof of Lemma 1.5. □

We also use the Möbius inversion formula.

LEMMA 1.6. *If* f,g *are functions from* $\mathbb{Z}^+$ *to* $\mathbb{C}$ *then*

$$f(n) = \sum_{d|n} g(d) \iff g(n) = \sum_{d|n} f(d)\, \mu(\tfrac{n}{d}) ,$$

where μ *is defined as follows:*

$$\mu(1) = 1. \text{ If } n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}, \alpha_i \geq 1, p_i \text{ prime, then}$$

$$\mu(n) = (-1)^k \text{ if } \alpha_1 = \ldots = \alpha_k = 1$$

$$= 0 \text{ otherwise.}$$

PROOF. Apostol [1], p. 32.

LEMMA 1.7. *The number of monic irreducible polynomials of degree* k *over* $\mathbb{F}_q$ *is given by*

$$\pi(k) = k^{-1} \sum_{d|k} \mu(\tfrac{k}{d})\, q^d, \text{ where}$$

μ is the Möbius function of Lemma 1.6.

PROOF. Blake and Mullin [2], p. 33.

3. BLOCK CIRCULANT MATRICES

We now consider block circulant matrices, which appear in various contexts in chapter 2.

An ordinary circulant is a matrix of the form

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_n \\ a_n & a_0 & \cdots & a_{n-1} \\ \vdots & & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix} = \wp(a_0, \ldots, a_n) .$$

where each a_i belongs to a field F.

DEFINITION 1.8. An (n,k)-block circulant is an $n \times n$ circulant whose entries are $(n,k-1)$-block circulants. An $(n,1)$-block circulant is an ordinary circulant.

A block circulant is usually defined in a wider sense (Davis [6], p. 176). Our definition corresponds to that of a circulant of level k ([6], p. 188) where the blocks have restrictions on their dimensions.

DEFINITION 1.9. The polynomial $f_A(x_1,\ldots,x_k)$ associated with the (n,k)-block circulant A is given by $f_A(x_1,\ldots,x_k) = \sum_{j=0}^{n-1} f_j x_k^j$, where $f_j(x_1,\ldots,x_{k-1})$ is the polynomial associated with the $(n,k-1)$ block circulant A_j, where $A = \wp(A_0,\ldots,A_{n-1})$. If $k = 1$, then $f_A(x) = \sum_{j=0}^{n-1} a_j x^j$.

For an ordinary circulant, the determinant was found by Ore [34], when char $F = 0$, or for char $F = p$, $(n,p) = 1$, and by Silva [40], when $(n,p) \neq 1$. The block case has been considered by Friedman [12], Chao [5], Smith [41] and Trapp [42].

THEOREM 1.1. *The eigenvalues of the block circulant* A *associated with* $f_A(x_1,\ldots,x_k)$ *are the values of* f_A *on all* k*-tuples of n'th roots of unity* λ_i *in a suitable extension field of* F.

PROOF. Consider first the case char $F = 0$, or $(n,p) = 1$. We consider A as an element of the group ring FG, where G is the direct sum of k copies of C_n, the cyclic group of order n. By Maschke's theorem, FG is semisimple, and the regular representation is equivalent to a direct sum of irreducible representations. If

F' is an extension field of F containing the n'th roots of unity, over F' the irreducible representations of G are one-dimensional, as G is abelian, and are the irreducible characters of G, defined by $\chi(g_i) = \lambda$, where g_i is a generator of a copy of C_n, and λ is any n'th root of unity. Since $A = f_A(T_1,\ldots,T_k)$, where T_i is associated with x_i, by linearity of the characters A is equivalent under linear transformations over F' to the matrix diag $\{f_A(\lambda_1,\ldots,\lambda_k)\}$, and so the eigenvalues are given by $\{f_A(\lambda_1,\ldots,\lambda_n)\}$. □

This equivalence also yields

<u>COROLLARY 1</u>. *The determinant of* A *is* $\Pi f_A(\lambda_1,\ldots,\lambda_k)$, where λ_i, $1 \le i \le k$, *ranges over all* k-*tuples of* n*'th roots of unity.*

<u>COROLLARY 2</u>. A *is invertible* $\Leftrightarrow f_A(\lambda_1,\ldots,\lambda_k) \neq 0$ *for any* k-*tuple of* n*'th roots of unity.*

We now assume $(n,p) \neq 1$. We use the following theorem of Silva [40], also proved in Chao [5].

<u>THEOREM 1.2</u>. *Let* $A = \wp(A_0,\ldots,A_{n-1})$, *where the* A_i *are square matrices of order* $n \ge 1$. *Let* $n = p^t m$, $p \nmid m$. *Then* $\det A \equiv (\det D)^{p^t} \bmod p$ *where* $D = \wp(D_0,\ldots,D_{m-1})$ *and* $D_r = \sum_{s=0}^{p^t-1} A_{sm+r}$, $0 \le r \le m-1$.

Applying this result, we see that Theorem 1.1 still holds, where each root is taken with multiplicity p^t.

The proof of Theorem 1.1 also provides the following result.

<u>THEOREM 1.3</u>. *If* $(n,p) = 1$, *then the rank of the block circulant matrix* A *is the number of non-zero eigenvalues of* A.

CHAPTER 2

PROPERTIES OF POLYNOMIALS OVER FINITE FIELDS

In this chapter we deal with various results concerning polynomials in one or several variables, defined over a finite field $\mathbb{F}_q$. Most of the results concern the distribution of the values taken by the polynomials. Of particular interest are polynomials whose value sets are uniformly distributed.

In the single-variable case the classical examples of such polynomials are the power polynomials and the Dickson polynomials. We consider polynomials of the form $(x^n - 1)/(x - 1)$ and Chebyshev polynomials of the second kind. We then consider various results on multivariable polynomials. These often extend known results or generalise results from the single variable case. We conclude with some results on the elementary symmetric functions over a finite field.

1. PERMUTATION POLYNOMIALS AND ORTHOGONAL SYSTEMS

DEFINITION 2.1. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial over $\mathbb{F}_q$ if the mapping $a \to f(a)$, $a \in \mathbb{F}_q$, is a permutation of $\mathbb{F}_q$.

DEFINITION 2.2. A polynomial vector $(f_1(x_1,\ldots,x_k), \ldots, f_k(x_1,\ldots,x_k))$, $f_i \in \mathbb{F}_q[x_1,\ldots,x_k]$, is called a permutation polynomial vector over $\mathbb{F}_q$ if the corresponding mapping $(a_1,\ldots,a_k) \to (f_1(a_1,\ldots,a_k),\ldots,f_k(a_1,\ldots,a_k))$ is a permutation of $\mathbb{F}_q^k$.

Permutation polynomial vectors have been studied in [8], [24], [29], [30], [31], and [33]. They are also discussed in [19].

DEFINITION 2.3. A polynomial vector $(f_1(x_1,\dots,x_k),\dots,f_r(x_1,\dots,x_k))$, $f_i \in \mathbb{F}_q[x_1,\dots,x_k]$, $r \le k$, is called an orthogonal system over $\mathbb{F}_q$ if the equation $(f_1(x_1,\dots,x_k),\dots,f_r(x_1,\dots,x_k)) = (a_1,\dots,a_r)$ has precisely q^{k-r} solutions for each $(a_1,\dots,a_r) \in \mathbb{F}_q^r$.

An orthogonal system consisting of one polynomial in k variables, ($r = 1$) is also called a permutation polynomial in k variables, and clearly a permutation polynomial vector is an orthogonal system. It was shown by Niederreiter [30] that any orthogonal system $f_1,\dots,f_r$, in k variables, $r \le k$, may be extended for each s with $r \le s \le k$, to an orthogonal system $f_1,\dots,f_s$ in k variables.

2. SINGLE VARIABLE POLYNOMIALS

We consider firstly single-variable polynomials. Many results on permutation polynomials appear in chapter 5 of Dickson [8], where a list is given of all permutation polynomials of a degree less than 6. Dickson introduced an important class of permutation polynomials, now known as Dickson polynomials, which are related to the classical Chebyshev polynomials of the first kind.

DEFINITION 2.4. The polynomial $g_k(x,a)$ defined by

$$g_k(x,a) = \sum_{t=0}^{[k/2]} \frac{k}{k-t} \binom{k-t}{t} (-a)^t x^{k-2t}$$

is called a Dickson polynomial.

If $t_k(x)$ is the Chebyshev polynomial of the first kind, then $g_k(x,a) = 2(\sqrt{a})^k\ t_k(x/2\sqrt{a})$.

THEOREM 2.1. $g_k(x,a)$ *is a permutation polynomial over* $\mathbb{F}_q$ *if and only if* $(k,q^2 - 1) = 1$.

PROOF. Lausch and Nöbauer [19], p. 209.

Later in this chapter, we will consider multivariable analogues of Dickson polynomials. An important property of the polynomials $g_k(x;1)$ relates to composition $\circ$ of polynomials (for a proof see [19] p. 211).

THEOREM 2.2. $g_k(x,1) \circ g_\ell(x,1) = g_{k\ell}(x,1)$.

This property will also generalise to the multivariable case. It ensures that the set of selfmaps of $\mathbb{F}_q$ induced by $\{g_k(x,1): k \in \mathbb{Z}\}$ forms a group. This and similar groups will be considered in later chapters.

The only classes of single-variable polynomials whose permutation behaviour is fully determined are the Dickson polynomials and the cyclic polynomials defined below.

DEFINITION 2.5. A cyclic polynomial is a polynomial of the form $ax^k + b$, $a \neq 0$, $k \in \mathbb{Z}^+$.

THEOREM 2.3. $ax^k + b$, $a,b \in \mathbb{F}_q$, $a \neq 0$ *is a permutation polynomial over* $\mathbb{F}_q$ *if and only if* $(k,q - 1) = 1$.

PROOF. From the fact that $\mathbb{F}_q^*$ is cyclic of order $q-1$.

We now give a full analysis of the permutation behaviour of another class of polynomials. To do so we use the criterion of Hermite ([19], p. 191).

PROPOSITION 2.1. *A polynomial* $f \in \mathbb{F}_q[x]$, $q = p^e$, *is a permutation polynomial over* $\mathbb{F}_q$ *if and only if*

(i) f *has exactly one root in* $\mathbb{F}_q$;

(ii) *the reduction of* $f^t \bmod (x^q - x)$, $0 < t < q - t$, $t \not\equiv 0 \bmod p$, *has degree less than or equal to* $(q - 2)$.

THEOREM 2.4. *The polynomial* $h_k(x) = 1 + x + x^2 + \ldots + x^k$ *is a permutation polynomial over* $\mathbb{F}_q$ *if and only if* $k \equiv 1 \bmod p(q - 1)$.

PROOF. Suppose $k \equiv 1 \bmod p(q - 1)$. Then $k = \alpha p(q - 1) + 1$, for some $\alpha \in \mathbb{Z}$, $\alpha \geq 0$. If $x \neq 1$, $h_k(x) = (x^{\alpha p(q-1)+2} - 1)/(x - 1) = (x^2 - 1)/(x - 1) = (x + 1)$. If $x = 1$, $h_k(x) = (k + 1) = 2$. Thus $h_k(x) = x + 1$, for all $x \in \mathbb{F}_q$, and so $h_k(x)$ is a permutation polynomial over $\mathbb{F}_q$.

We now consider the problem of showing that the given condition is a necessary one. We note that if $k \equiv \ell \bmod p(q - 1)$ then $h_k(x) = h_\ell(x)$ for all $x \in \mathbb{F}_q$. Thus it suffices to consider $k < p(q - 1)$. If $k \geq (q - 1)$ then in the reduction of $h_k(x) \bmod (x^q - x)$ the coefficient of x^{q-1} is $\left[\frac{k}{q-1}\right]$ which is not zero mod p, and so $h_k(x)$ is not a permutation polynomial by Proposition 2.1. Thus we may assume that $k < (q - 1)$.

We begin with the case $q = p$. We consider $[h_k(x)]^t$, where $t = \left[\frac{p-1}{k}\right] + 1$, $k \geq 2$. The terms which reduce to x^{p-1} are those of the form $x^{\alpha(p-1)}$, $\alpha \in \mathbb{Z}$, $\alpha > 0$. The degree of $[f_k(x)]^t$ is kt. We may suppose that k does not divide $(p - 1)$. Let $(p - 1) = \alpha k + \beta$, $0 < \beta < k$, $\alpha \geq 1$. Then $t = \alpha + 1$ and $kt = (\alpha + 1)k = (p - 1) + (k - \beta)$. Since $(k - \beta) < (p - 1)$, $kt < 2(p - 1)$. Thus we need only consider the term x^{p-1}. Since $[h_k(x)]^t$ is symmetric, the coefficient of x^{p-1} equals the coefficient of $x^{kt-(p-1)}$, and $kt - (p - 1) = (k - \beta) < k$. We show that if $r \leq k$, the coefficient of x^r in $[h_k(x)]^t$ is $\binom{r+t-1}{t-1}$. This is established by induction on t. If $t = 1$ the result holds. If it holds for $t = t_0$, then $[h_k(x)]^{t_0} = \sum_{r=0}^{k} \binom{r+t_0-1}{t_0-1} x^r$ + terms of higher degree. Then $[h_k(x)]^{t_0+1} = h_k(x)\,[h_k(x)]^{t_0}$ and the coefficient of x^r is $\sum_{\ell=0}^{r} \binom{\ell+t_0-1}{t_0-1} = \binom{r+t_0}{t_0}$. If $n \geq s$ and $n < p$, $s < p$, then $\binom{n}{s} \not\equiv 0 \bmod p$, (from the explicit form of $\binom{n}{s}$). We show that $\binom{r+t-1}{t-1} \not\equiv 0 \bmod p$ when $r = kt - (p - 1)$. Clearly $(t - 1) = \left[\frac{p-1}{k}\right] < p$ so we need only show that $(r + t - 1) < p$ or that $(k + 1)t - 1 < (2p - 1)$. $(k + 1)t - 1 = (k + 1)(\alpha + 1) - 1 = \alpha k + \alpha + k$. Since $\alpha k = (p - 1) - \beta < (p - 1)$, the result holds unless $(\alpha + k) > p$. Then $\alpha k < (p - 1)$ and $(\alpha + k) > p$. As $\alpha, k \in \mathbb{Z}$, graphical considerations show that no such α,k can exist.

We now consider the case where $q = p^e > p$. We proceed by induction on e. If $h_k(x)$ is a permutation polynomial over $\mathbb{F}_{p^e}$ then it is over $\mathbb{F}_{p^{e-1}}$. Thus $k \equiv 1 \bmod p(p^{e-1} - 1)$. Let $k = \alpha p(p^{e-1}) + 1$,

$\alpha \in \mathbb{Z}$, $\alpha \geq 1$. We may assume that $k < (q - 1)$, or that $\alpha p(p^{e-1} - 1) + 1 < p^e - 1$. This implies $\alpha < 2$, so in fact $\alpha = 1$. We consider $[h_k(x)]^2$, with $k = p(p^{e-1} - 1) + 1$.

If $p = 2$, then $k = q - 1$, and so $h_k(x)$ is not a permutation polynomial. Thus assume $p > 2$. Then $k < (q - 1)$ and $\deg\,[(h_k(x)]^2 = 2\{p(p^{e-1} - 1) + 1\} > (p^e - 1)$. The coefficient of x^{q-1} equals the coefficient of $x^{2k-(q-1)}$, which is $2k - q + 2 = 2p(p^{e-1} - 1) - p^e + 4$. Since $p > 2$, this is non-zero mod p, and so $h_k(x)$ is not a permutation polynomial over $\mathbb{F}_q$. $\square$

If we define the polynomial $h(1,1,k)(x) \doteq x(1 + x + x^2 + \ldots + x^k)$, then $h(1,1,k)$ is a permutation polynomial if and only if $k + 1 \equiv 1 \bmod p(q - 1)$. As a generalisation of this we propose the following conjecture. Let $h(\ell,j,k)(x) = x^{\ell}(1 + x^j + \ldots + (x^j)^k)$. Then if $((\ell,j),q - 1) > 1$, $h(\ell,j,k)$ is not a permutation polynomial over $\mathbb{F}_q$. Assume $(\ell,j) = 1$. Let $J = \{x \in \mathbb{F}_q : x^j = 1\}$. Then we have

<u>CONJECTURE</u>. $h(\ell,j,k)$, $\ell > 0, j > 0$, is a permutation polynomial over $\mathbb{F}_q$ if and only if

$$\begin{cases} k + 1 \equiv 1 \bmod \dfrac{q - 1}{(j,q - 1)} \quad \text{and} \quad (\ell,q - 1) = 1 \\ \text{and } (k + 1) \in J \end{cases}$$

or

$$\begin{cases} k + 1 \equiv -1 \bmod \dfrac{q - 1}{(j,q - 1)} \text{ and } (\ell - j,q - 1) = 1 \\ \text{and } (k + 1) \in -J. \end{cases}$$

In the first case, if $x^j \neq 1$, $h(\ell,j,k)(x) = x^{\ell}\left\{\dfrac{x^{j(k+1)} - 1}{x^j - 1}\right\} = x^{\ell}$.

If $x^j = 1$, $h(\ell,j,k)(x) = (k + 1)x^\ell$. Since $(\ell,q - 1) = 1$, the polynomial x^ℓ permutes $\mathbb{F}_q$. Since $(\ell,j) = 1, x^\ell$ maps $\mathbb{F}_q\backslash\{J\}$ to itself, as x^ℓ permutes J. Since $(k + 1) \in J$, the polynomial $(k + 1)x^\ell$ permutes J, and so $h_k(x)$ permutes $\mathbb{F}_q$.

In the second case, if $x \notin J$, $h_k(x) = x^\ell \dfrac{x^{-j} - 1}{x^j - 1} = -x^{\ell-j}$.

If $x \in J$, $h_k(x) = (k + 1)x^\ell$. The image of J under $-x^{\ell-j}$ is $-J$. Thus $h_k(x)$ maps $\mathbb{F}_q\backslash J \to \mathbb{F}_q\backslash(-J), x^\ell$ permutes J, and $(k + 1)x^\ell : J \to -J$ since $(k + 1) \in -J$.

The question as to whether these are the only permutation polynomials of this type remains open unless $\ell = j = 1$. If $(\ell,q - 1) = (j,q - 1) = 1$, this conjecture would imply that $k + 1 \equiv 1 \bmod p(q - 1)$ is a necessary condition. For q prime, $q \leq 17$, the conjecture has been verified by computation.

<u>DEFINITION 2.6</u>. The Chebyshev polynomial of the second kind, $f_k(x)$ is defined by $f_k(x) = \sum_{i=0}^{[k/2]} \binom{k-i}{i}(-1)^i x^{k-2i}$.

For these Chebyshev polynomials of the second kind, $f_k(x)$, $k \in \mathbb{Z}$, we can find conditions sufficient to ensure that $f_k(x)$ is a permutation polynomial when q is odd.

If the transformation $x = u + u^{-1}$ is made, then we have $f_k(x) = (u^{k+1} - u^{-(k+1)})/(u - u^{-1})$ if $u \neq \pm 1$, $f_k(2) = (k + 1) \bmod p$, $f_k(-2) = (-1)^k(k + 1) \bmod p$.

The polynomials which we describe below induce permutations of $\mathbb{F}_q$ of a special type.

DEFINITION 2.7. A map $\pi: \mathbb{F}_q \to \mathbb{F}_q$ is called an $\mathcal{S}$-permutation if

(i) $\pi(-a) = -\pi(a)$, for each $a \in \mathbb{F}_q$

and (ii) $\pi(a) = a$ or $-a$, for each $a \in \mathbb{F}_q$.

We have the following immediate consequences of the definition.

1. Every $\mathcal{S}$-permutation of $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$.
2. The identity map is an $\mathcal{S}$-permutation.
3. Every $\mathcal{S}$-permutation fixes 0.
4. The set of $\mathcal{S}$-permutations of $\mathbb{F}_q$ is closed under composition.
5. There are $2^{\frac{1}{2}(q-1)}$ distinct $\mathcal{S}$-permutations of $\mathbb{F}_q$.
6. If π is an $\mathcal{S}$-permutation then $\pi \circ \pi = 1_{\mathbb{F}_q}$.

Example. In $\mathbb{F}_5$, the map

$$0 \to 0,\ 1 \to 1,\ -1 \to -1,\ 2 \to -2,\ -2 \to 2,$$

defines an $\mathcal{S}$-permutation.

THEOREM 2.5. *If* k *satisfies the three congruences*

$$k + 1 \equiv \pm 2 \bmod p$$
$$k + 1 \equiv \pm 2 \bmod \tfrac{1}{2}(q - 1)$$
$$k + 1 \equiv \pm 2 \bmod \tfrac{1}{2}(q + 1)$$

and q *is odd then* $f_k(x)$ *induces an* $\mathcal{S}$*-permutation of* $\mathbb{F}_q$.

PROOF. We note firstly that if M is the subset of $\mathbb{F}_{q^2}$ consisting of all solutions of equations of the form $x^2 - rx + 1 = 0$, $r \in \mathbb{F}_q$, then

$$M = \{u \in \mathbb{F}_{q^2}: u^{q-1} = 1 \text{ or } u^{q+1} = 1\} .$$

(This result may be found in the proof of theorem 9.43 in Lausch and Nöbauer [19], page 210). Since one of $\frac{1}{2}(q - 1)$, $\frac{1}{2}(q + 1)$ is even, k must be odd. Thus $f_k(x)$ consists of terms of odd degree. Thus $f_k(-x) = -f_k(x)$ and condition (i) of definition 2.6 is satisfied. To establish condition (ii), let $u \in \mathbb{F}_{q^2}$ with $u^2 - xu + 1 = 0$. If $u^{q-1} = 1$, then $u^{\frac{1}{2}(q-1)} = \pm 1$. If $u^{\frac{1}{2}(q-1)} = 1$, then since $k + 1 = \pm 2 \bmod \frac{1}{2}(q - 1)$, $u^{k+1} = u^2$ or $u^{k+1} = u^{-2}$. Thus $f_k(x) = (u^2 - u^{-2})/(u - u^{-1}) = u + u^{-1} = x$, or $f_k(x) = (u^{-2} - u^2)/(u - u^{-1}) = -(u + u^{-1}) = -x$. The case $u^{\frac{1}{2}(q-1)} = -1$ is similar, as is the case where $u^{q+1} = 1$. If $u = \pm 1$, then $f_k(2) = 2$ or -2. Thus $f_k(x)$ induces an $\mathcal{S}$-permutation on $\mathbb{F}_q$. □

COROLLARY. *If* k *satisfies the conditions of theorem 2.4, then* $f_k \circ f_k = x$, *where the left hand side is reduced* mod $(x^q - x)$.

We may express $\mathbb{F}_q$ as the disjoint union of five sets $A = \{2,-2\}$, $B_1 = \{x \in \mathbb{F}_q: x = u + u^{-1};\ u^{q-1/2} = 1\}\backslash A$, $B_2 = \{x \in \mathbb{F}_q: x = u + u^{-1};\ u^{q-1/2} = -1\}\backslash A$, $C_1 = \{x \in \mathbb{F}_q: x = u + u^{-1};\ u^{q+1/2} = 1\}\backslash A$, $C_2 = \{x \in \mathbb{F}_q: x = u + u^{-1};\ u^{q+1/2} = -1\}\backslash A$. Suppose q large (we consider small q later). The distinct maps of $\mathbb{F}_q$ are given by the conditions $k+1 \equiv \pm 2(p)$, $k + 1 \equiv 2, \frac{q-1}{2} - 2, \frac{q-1}{2} + 2, -2 \bmod (q-1)$, $k+1 \equiv 2, \frac{q+1}{2} - 2, \frac{q+1}{2} + 2, -2 \bmod (q + 1)$. Since precisely one of $(\frac{q-1}{2}, \frac{q+1}{2})$ is even, only eight of the sixteen possible combinations are consistent. This yields sixteen distinct maps. Suppose $\frac{q-1}{2}$ is odd. Then the conditions which are inconsistent are $k + 1 \equiv \frac{q-1}{2} \pm 2$. The maps induced on $\mathbb{F}_q$ may be calculated explicitly in both cases, the set of maps is closed under composition and the resulting group G is isomorphic to C_2^4.

For small q, the conditions may not all be distinct. Computer calculations yield the following special cases.

PROPOSITION 2.2. *Let* G *be the group of maps of* $\mathbb{F}_q$ *induced by the Chebyshev polynomials of the second kind described in theorem 2.5. Then*

$$G \simeq C_2 \text{ if } q = 3$$

$$G \simeq C_2^2 \text{ if } q = 5$$

$$G \simeq C_2^3 \text{ if } q = 7 \text{ or } q = 9$$

$$G \simeq C_2^4 \text{ if } q \geq 11.$$

3. POLYNOMIALS IN SEVERAL VARIABLES

We now consider various results on polynomials in several variables over $\mathbb{F}_q$. If $p(x_1,\ldots,x_k)$ is a polynomial over $\mathbb{F}_q$ it may be reduced mod $\{x_1^{q-1} - 1,\ldots,x_k^{q-1} - 1\}$ to yield a polynomial of degree less than (q - 1) in each variable. The reduced polynomial induces the same map of $\mathbb{F}_q^{*k} \to \mathbb{F}_q$ as $p(x_1,\ldots,x_k)$ does. In theorem 1.1, we take $n = q - 1$ to yield

THEOREM 2.5. *The number of zeros of* $f(x_1,\ldots,x_k)$ *which are such that* $x_i \neq 0$ *for* $1 \leq i \leq k$, *is given by* $(q - 1)^k - r$, *where* r *is the rank of* C_f, *the* (q - 1,k)*-block circulant associated with* f *reduced* mod $\{x_1^{q-1} - 1,\ldots,x_k^{q-1} - 1\}$.

PROOF. The $(q - 1)$st roots of unity in $\mathbb{F}_q$ are precisely the non-zero elements of $\mathbb{F}_q$, and by theorem 1.3 the rank of C_f is the number of non-zero eigenvalues of C_f. Thus the number of zeros of f is $(q - 1)^k - r$, since the dimension of C_f is $(q - 1)^k$. □

The case of $k = 1$ of theorem 2.5 is the classical König-Rados theorem, a proof of which may be found in McDonald [27] or Rédei [37]. Horakova and Schwarz [16], [38] and [39] have generalised the one-variable König-Rados theorem to obtain results on the factorisation of $f(x)$.

PROPOSITION 2.3. *(Horakova and Schwarz). Let* $f(x) \in \mathbb{F}_q[x]$ *be of degree less than* $q - 1$. *Then the number of different irreducible factors of* $f(x)$ *of degree* d *is given by*

$$\frac{1}{d} \sum_{k|d} \mu(\tfrac{d}{k})(q^k - 1 - r_k), \text{ where}$$

μ *is the Möbius function, and* r_k *is the rank of the* $(q^k - 1)$-*circulant associated with* f, *considered as a polynomial over* $\mathbb{F}_{q^k}$.

This generalises as follows:

THEOREM 2.6. *Let* L_d *be the subset of* $\mathbb{F}_q^n$ *defined by* $(\alpha_1,\ldots,\alpha_n) \in L_d$ *if and only if* $\gcd(\deg \alpha_1,\ldots,\deg \alpha_n) = d$ *and* $\alpha_j \neq 0$, *for* $1 \leq j \leq n$. *Then the number of zeros of* $p(x_1,\ldots,x_n) \in \mathbb{F}_q[x_1,\ldots,x_n]$ *which lie in* L_d *is given by*

$$\sum_{k|d} \mu(\tfrac{d}{k})(q^{kn} - 1 - r_k) ,$$

where r_k *is the rank of the block circulant associated with* p *as a polynomial in* $\mathbb{F}_{q^k}$.

PROOF. The number of zeros of p which lie in $\mathbb{F}^*_{q^k}$ is given by $q^{nk} - 1 - r_k$. If σ_i is the number of such zeros lying in L_i, then

$$\sum_{i|k} \sigma_i = q^{nk} - 1 - r_k \; .$$

By Möbius inversion, $\sigma_d = \sum_{k|d} \mu(\frac{d}{k})(q^{nk} - 1 - r_k)$. (lemma 1.6). □

Circulant matrices can be used to provide a necessary and sufficient condition for a polynomial to be a permutation polynomial. The one-variable case, due to Raussnitz [36] is as follows:

PROPOSITION 2.4. *The polynomial* $f(x)$ *of degree less than* $(q - 1)$ *is a permutation polynomial over* $\mathbb{F}_q$ *if and only if the characteristic polynomial* $\chi(\lambda)$ *of the* $(q - 1) \times (q - 1)$*-circulant associated with* f *is given by*

$$\chi(\lambda) = (\lambda^q - \lambda)/(\lambda - f(0)) \; .$$

PROOF. The eigenvalues of A are the set of $f(\alpha)$, $\alpha \in \mathbb{F}_q\backslash\{0\}$, and since $\prod_{\beta \in F_q} (\lambda - \beta) = \lambda^q - \lambda$, the result follows. □

(See also [7] vol. 3, page 290 and [43], page 191).

In the general case, it is not sufficient to consider the block circulant associated with f, since the variables must be allowed to take zero values. We construct a new matrix as follows: given $f(x_1,\ldots,x_k)$, form the block circulant associated with f, denoted A_0. Now substituting each variable in turn by zero, we obtain k polynomials in $(k - 1)$ variables, with associated block circulants $A_1^{(1)},\ldots,A_1^{(k)}$, and so on, next taking pairs of variables to be zero, etc. We then form the diagonal block matrix

$$A = \oplus \sum_{i=0}^{k-1} A_i^{(j)} .$$

The dimension of A is $(q-1)^k + \binom{k}{1}(q-1)^{k-1} + \ldots = q^k - 1$.

THEOREM 2.7. *The polynomial* $f(x_1,\ldots,x_k)$ *is a permutation polynomial if and only if the matrix* A *defined above satisfies the condition* $(\lambda - f(0,\ldots,0))\chi(A) = (\lambda^q - \lambda)^{q^{k-1}}$ *where* $\chi(A)$ *is the characteristic polynomial of* A.

PROOF. As in the one-variable case, using the fact that the characteristic polynomial of the direct sum is the product of the characteristic polynomials of its components. □

4. PERMUTATION POLYNOMIALS IN SEVERAL VARIABLES

The following result appears in Lidl and Niederreiter [24].

PROPOSITION 2.5. *The polynomial* $f(x_1,\ldots,x_n) = g(x_1,\ldots,x_m) + h(x_{m+1},\ldots,x_n)$, $1 \le m \le n$, *is a permutation polynomial over* $\mathbb{F}_p$, p *prime, if and only if at least one of* g *and* h *is a permutation polynomial.*

It is shown in [24] that there are polynomials g and h in disjoint sets of variables over $\mathbb{F}_q$, q not prime, such that neither g nor h are permutation polynomials when g + h is a permutation polynomial. The next result describes when this can occur. Let G denote the additive group of $\mathbb{F}_q$.

THEOREM 2.8. *Let* $f_1,\ldots,f_t$ *be polynomials in disjoint sets of variables, where* f_i *is a polynomial in* v_i *variables. Then* $f_1 +\ldots+ f_t$ *is a permutation polynomial over* $\mathbb{F}_q$, $q = p^e$, *if and only if, for any subgroup* H *of* G *of order* p^{e-1}, *there is an* f_i *which distributes* $(\mathbb{F}_q)^{v_i}$ *uniformly over the cosets of* H *in* G.

PROOF. We consider the group ring $\mathbb{C}G$. For each $g \in G$, let $M_g(f) = \text{Card}\ \{(x_1,\ldots,x_k) \in \mathbb{F}_q^k\colon f(x_1,\ldots,x_k) = g\}$, where $f \in \mathbb{F}_q[x_1,\ldots,x_k]$. Define a mapping ϕ from $\mathbb{F}_q[x_1,\ldots,x_k]$ to $\mathbb{C}G$ by $\phi = f \to \sum M_g(f)g \in \mathbb{C}G$. Let $e = \sum\limits_{g\in G} g$. Then f is a permutation polynomial over $\mathbb{F}_q$ if and only if $\phi(f) = ke$ for some $k \in \mathbb{Z}$. Further, if f,h are polynomials in disjoint sets of variables, then $\phi(f + h) = \phi(f).\phi(h)$.

Let H be a subgroup of G of index p and let $\theta = G \to G/H \simeq C_p$, where C_p is the cyclic group of order p. Then θ extends to a homomorphism $\theta = \mathbb{C}G \to \mathbb{C}C_p$, and $\mu = \theta \circ \phi$ maps $\mathbb{F}_q[x_1,\ldots,x_k]$ into $\mathbb{C}C_p$. Then the condition of the theorem may be stated as follows. For each subgroup H of G of index p there is an f_i with $\mu(f_i) = k\bar{e}$, for some $k \in \mathbb{Z}$, where $\bar{e} = \sum g \in \mathbb{C}C_p$ and the summation is over all elements of C_p.

Now suppose that $f_1 +\ldots+ f_t$ is a permutation polynomial then $\phi(f_1 +\ldots+ f_t) = ke$, $k \in \mathbb{Z}$. Let H be a subgroup of G of index p, and let μ,θ be the corresponding maps defined above. Then

$\mu(f_1) \ldots \mu(f_t) = k\theta(e) = k_1\bar{e}$. If g is a generator of C_p, and $\chi\colon C_p \to \mathbb{C}$ is the character defined by $\chi(p) = \zeta$, ζ a primitive p'th root of unity, then $\chi(\bar{e}) = 0$. Thus $\chi(\mu(f_i)) = 0$ for some i. If $\mu(f_i) = \sum_{t=0}^{p-1} \alpha_t g^t$, where $\alpha_i \in \mathbb{Z}$, then $\chi(\mu(f_i)) = \sum_{t=0}^{p-1} \alpha_t g^t = 0$. Since the minimal polynomial of ζ is the cyclotomic polynomial $\phi_p(x)$, which has degree p - 1, $\phi_p(x)$ divides $\sum_{t=0}^{p-1} \alpha_t x^t$ in $\mathbb{C}[x]$. As the degrees of these polynomials are equal, they differ only by a constant multiple, and so $\mu(f_i) = k_2\phi_p(g) = k_2\bar{e}$ for some $k_2 \in \mathbb{Z}$, and so f_i satisfies the condition of the theorem. Conversely, any irreducible character χ of $G(= C_p^e)$ may be represented in the form $G \overset{\theta}{\to} C_p \overset{\psi}{\to} \mathbb{C}$ where ψ maps $g \in C_p$ to ζ, and θ is a homomorphism. Thus if χ is a non-principal character of G, then

$$\begin{aligned}\chi(\phi(f_1 + \ldots + f_t)) &= \chi(\phi(f_1)) \ldots \chi(\phi(f_t)) \\ &= (\psi \circ \mu)(f_1) \ldots (\psi \circ \mu)(f_t) = 0, \text{ since } \psi(k\bar{e}) = 0.\end{aligned}$$

So in the representation of $\mathbb{C}G$ as a direct sum of one-dimensional subspaces, the only non-zero component of $\phi(f_1 + \ldots + f_t)$ is the one corresponding to the principal character. Hence $\phi(f_1 + \ldots + f_t)$ belongs to the subspace of $\mathbb{C}G$ corresponding to the principal character. Since $\chi(e) = 0$ if $\chi \neq \chi_1$, and $\chi_1(e) \neq 0$, it follows that $\phi(f_1 + \ldots + f_t) = ke$, $k \in \mathbb{Z}$, and so $(f_1 + \ldots + f_t)$ is a permutation polynomial over $\mathbb{F}_q$. □

If q = p, then we obtain proposition 2.5, since then H = {1}, $G/H \simeq G$, and the condition on f_i reduces to f_i being a permutation polynomial over $\mathbb{F}_q$.

The following result generalises a theorem of Niederreiter [31] from the prime case. Let $\theta\colon GR(q^{k-1},r) \to GR(p,r)(\simeq \mathbb{F}_q, q = p^r)$, be the canonical map with kernel (p), where $GR(q^t,r)$ is a Galois ring as defined in chapter 1. Let A be a set of representatives of the inverse images of θ, and let $\theta(a') = a$, $a \in \mathbb{F}_q$, $a' \in A$.

THEOREM 2.9. *Let* $f \in \mathbb{F}_q[x_1,\dots,x_k]$. *Then* f *is a permutation polynomial over* $\mathbb{F}_q$ *if and only if* $f(x_1,\dots,x_k) = a$, $a \in \mathbb{F}_q$, *has a solution and* $\sum_{(a_1,\dots,a_k)\in A^k} [f(a_1,\dots,a_k)]^{tp^{(r(k-1)-1)}} = 0$ *in* $GR(q^{k-1},r)$ *for* $t = 1,\dots,q-1$, *where* A *and* $GR(q^{k-1},r)$ *are given above.*

PROOF. Let $k_a = \text{card}\,\{(x_1,\dots,x_k) \in \mathbb{F}_q^k\colon f(x_1,\dots,x_k) = a\}$ for $a \in \mathbb{F}_q$. If $\theta(x) = \theta(y)$ for $x,y \in GR(q^{k-1},r)$, then $x = y + p\alpha$, $\alpha \in GR(q^{k-1},r)$, so

$$x^{p^{(r(k-1)-1)}} = y^{p^{(r(k-1)-1)}}$$

Thus
$$\sum_{(a_1,\dots,a_k)\in A^k} [f(a_1,\dots,a_k)]^{tp^{(r(k-1)-1)}}$$

$$= \sum_{a\in\mathbb{F}_q} k_a (a')^{tp^{(r(k-1)-1)}}.$$

Since $k_a = q^{k-1}$, this sum is zero in $GR(q^{k-1},r)$. Conversely, if the conditions of the theorem hold, then $\sum_{a\in\mathbb{F}_q} k_a (a')^{tp^{(r(k-1)-1)}} = 0$ in $GR(q^{k-1},r)$, for $t = 1,\dots,q-1$. This also holds for $t = 0$. Regarding the $\{k_a\}$ as variables, we obtain a system of equations in

$\{k_a\}$. The coefficient matrix has determinant

$$D = \prod_{\substack{a_i', a_j' \in A \\ i \neq j}} ((a_i')^{p^{(r(k-1)-1)}} - (a_j')^{p^{(r(k-1)-1)}}).$$

$\theta(D) \neq 0$ in $\mathbb{F}_q$ so $D \notin (p)$ in $GR(q^{k-1},r)$. Thus $k_a = 0$ in $GR(q^{k-1},r)$, and since $k_a \in \mathbb{Z}$, $k_a \equiv 0 \bmod q^{k-1}$ for all $a \in \mathbb{F}_q$. But $k_a \geq 1$ for all $a \in \mathbb{F}_q$, and so $k_a \geq q^{k-1}$. Since $\sum_{a \in \mathbb{F}_q} k_a = q^k$, $k_a = q^{k-1}$, and so f is a permutation polynomial over $\mathbb{F}_q$. □

5. κ-POLYNOMIALS

We now consider a more general class of polynomials, known as κ-polynomials.

DEFINITION 2.8. A polynomial $f(x_1,\ldots,x_k)$ is called a κ-polynomial over $\mathbb{F}_q$ if $k_a = \text{card}\,\{(x_1,\ldots,x_k) \in \mathbb{F}_q^k\colon f(x_1,\ldots,x_k) = a\}$, $a \in \mathbb{F}_q$, is independent of a for $a \neq 0$.

In the single variable case, a κ-polynomial is a permutation polynomial or induces the zero map on $\mathbb{F}_q$. We shall later give examples of κ-polynomials in several variables which are not permutation polynomials. Suppose that f,g are polynomials in disjoint sets of variables. Suppose further that f is a κ-polynomial and $f(x_1,\ldots,x_k) = a$ has m solutions for $a \neq 0$. Let g be a polynomial in ℓ variables with t zeros. Then $fg = a$ has $m(q^\ell - t)$ solutions if $a \neq 0$. Thus fg is a κ-polynomial.

If f_1, f_2 are κ-polynomials in disjoint sets of variables, and if the equation $f = a$ has m_f solutions for $a \neq 0$, then $m_{f_1 f_2} = m_{f_1} m_{f_2}$. An analogue of theorem 2.8 may be obtained as follows. Let g be a fixed generator of $\mathbb{F}_q \setminus \{0\}$. Let θ: $f \to \sum_{t=0}^{q-2} c_t x^t$, where $c_t = \text{card}\,\{f = g^t\}$, and $\theta(f) \in \mathbb{Z}[x]/(x^{q-1} - 1)$. Then if f_1, f_2 are polynomials in disjoint sets of variables, $\theta(f_1\ f_2) = \theta(f_1)\ (f_2)$. If $f_1, \ldots, f_t$ are polynomials in disjoint sets of variables then $f_1, \ldots, f_t$ is a κ-polynomial over $\mathbb{F}_q$ if and only if $\theta(f_1, \ldots, f_t) = m \left(\frac{x^{q-1} - 1}{x - 1} \right)$ for some $m \in \mathbb{Z}$. For example, suppose $q = 5$, $f_1 = a$, $a \neq 0$, has m_1 solutions if $a = 1$ or $a = g$, and no solutions otherwise. Suppose $f_2 = a$ has m_2 solutions for $a = 1$, $a = g^2$, and no solutions otherwise. Then

$$\theta(f_1 f_2) = m_1 m_2 (1 + x)(1 + x^2) = m_1 m_2 \left(\frac{x^4 - 1}{x - 1} \right),$$ and so $f_1 f_2$ is a κ-polynomial, even though q is prime, in contrast to theorem 2.4.

The following result is an analogue of a criterion of Niederreiter [29]. Let χ be a character of the multiplicative group F_q^* and define $\chi(0) = 0$.

<u>THEOREM 2.10</u>. $f(x_1, \ldots, x_k)$ *is a* κ*-polynomial over* $\mathbb{F}_q$ *if and only if* $\sum_{(a_1, \ldots, a_k) \in \mathbb{F}_q^k} \chi(f(a_1, \ldots, a_k)) = 0$ *for all non-principal characters* χ *of* $\mathbb{F}_q^*$.

PROOF. $$\sum_{(a_1,\ldots,a_k)\in\mathbb{F}_q^k} \chi(f(a_1,\ldots,a_k)) = \sum_{a\in\mathbb{F}_q} k_a\chi(a)$$

$$= k \sum_{a\in\mathbb{F}_q} \chi(a)$$

$$= 0 .$$

Conversely, if $a \neq 0$,

$$k_a = \frac{1}{(q-1)} \sum_{(a_1,\ldots,a_k)} \sum_{\chi} \chi\left(\frac{f(a_1,\ldots,a_k)}{a}\right)$$

where χ runs over all characters of $\mathbb{F}_q^*$.

Thus $$k_a = \frac{1}{(q-1)} \sum_{(a_1,\ldots,a_k)} \sum_{\chi} \chi(f(a_1,\ldots,a_k))\chi^{-1}(a)$$

$$= \frac{1}{q-1} \sum_{\chi} \chi^{-1}(a) \sum_{(a_1,\ldots,a_k)} \chi(f(a_1,\ldots,a_k))$$

$$= \frac{1}{q-1} \sum_{\chi=1} \chi^{-1}(a) \sum_{(a_1,\ldots,a_k)} \chi(f(a_1,\ldots,a_k))$$

Let $T = \text{card }\{(a_1,\ldots,a_k)\colon f(a_1,\ldots,a_k) \neq 0\}$.

Then $k_a = \frac{1}{q-1}(1.T) = \frac{T}{q-1}$, and so f is a κ-polynomial. □

6. ELEMENTARY SYMMETRIC FUNCTIONS

To conclude this chapter we consider the elementary symmetric functions over $\mathbb{F}_q$. We shall prove that some of these are κ-polynomials, and even permutation polynomials. We denote the elementary symmetric function of degree r in n variables by S_r^n. We begin with the following result on homogeneous polynomials.

THEOREM 2.11. *If* $f(x_1,\ldots,x_k)$ *is homogeneous of degree* r, *and* $(r,q-1) = 1$, *then* f *is a* κ*-polynomial over* $\mathbb{F}_q$.

PROOF. If $f(x_1,\ldots,x_k) = 0$ for all $(x_1,\ldots,x_k) \in \mathbb{F}_q^k$ then f is a κ-polynomial. Suppose that $f(x_1,\ldots,x_k) = \alpha(\neq 0)$ for some $(x_1,\ldots,x_k) \in \mathbb{F}_q^k$. Let $\beta \in \mathbb{F}_q$, $\beta \neq 0$. Then since x^r is a permutation polynomial over $\mathbb{F}_q$, there exists a unique $\lambda \in \mathbb{F}_q$ with $\lambda^r = \alpha^{-1}\beta$. Then $f(\lambda x_1,\ldots,\lambda x_k) = \beta$, and the map $(x_1,\ldots,x_k) \to (\lambda x_1,\ldots,\lambda x_k)$ is a bijection of the sets $\{(x_1,\ldots,x_k)\colon f(x_1,\ldots,x_k) = \alpha\}$ and $\{(x_1,\ldots,x_k)\colon f(x_1,\ldots,x_k) = \beta\}$. Thus f is a κ-polynomial. □

We note that the condition of theorem 2.11 is not a necessary condition, since $f(x_1,\ldots,x_k) = x_1 \ldots x_k$ is a κ-polynomial, where k is arbitrary.

However, we do have

PROPOSITION 2.6. *If* $f(x_1,\ldots,x_n)$ *is homogeneous of degree* r *then a necessary condition for* f *to be a permutation polynomial over* $\mathbb{F}_q$ *is that* $(r,q-1) = 1$.

PROOF. If $t = (r,q-1)$, then there are t solutions to $\alpha^t = 1$, Then $f(\alpha x_1,\ldots,\alpha x_n) = f(x_1,\ldots,x_n)$. Thus if $f(x_1,\ldots,x_n) = 1$, so is $f(\alpha x_1,\ldots,\alpha x_n)$. Thus the cardinality of the solution set of $f(x_1,\ldots,x_n) = 1$ is divisible by t, and so $t = p^k$. Thus $t = 1$. □

We use the following lemma to locate some permutation polynomials among the elementary symmetric functions. Define $f^{(s)}_{(x_1,\ldots,x_n)}\colon \mathbb{F}_q \to \mathbb{F}_q$ by $f^{(s)}_{(x_1,\ldots,x_n)}(\lambda) = S(x_1+\lambda,\ldots,x_n+\lambda)$, for any polynomial S in n variables over $\mathbb{F}_q$, and any $(x_1,\ldots,x_n) \in \mathbb{F}_q^n$.

<u>LEMMA 2.1</u>. *If* $f^{(s)}_{(x_1,\ldots,x_n)}(\lambda)$ *is a permutation polynomial in* λ *over* $\mathbb{F}_q$ *for any choice of* $(x_1,\ldots,x_n) \in \mathbb{F}_q^n$, *then* S *is a permutation polynomial in* $(x_1,\ldots,x_n)$ *over* $\mathbb{F}_q$.

<u>PROOF</u>. Define an equivalence relation ρ on $\mathbb{F}_q^n$ by $(x_1,\ldots,x_n)$ $\rho(x_1',\ldots,x_n')$ if and only if there exists $\alpha \in \mathbb{F}_q$ such that $x_i' = x_i + \alpha$, for $1 \le i \le n$. Each equivalence class contains q elements and there are q^{n-1} classes. For each $(x_1,\ldots,x_n)$, $S(x_1+\lambda,\ldots,x_n+\lambda) = \beta$, $\beta \in \mathbb{F}_q$, has a unique solution λ. Thus there is a unique solution in each ρ-class. Since there are q^{n-1} classes, $S(x_1,\ldots,x_n)$ is a permutation polynomial. □

The converse of this lemma does not hold, even for homogeneous symmetric functions. For example, $S(x_1,x_2,x_3) = x_1^3 + x_2^3 + x_3^3$ is a permutation polynomial over $\mathbb{F}_3$, but $f^{(s)}_{(x_1,x_2,x_3)}(\lambda) = x_1^3 + x_2^3 + x_3^3$ is a constant function in λ.

In order to prove some permutation polynomial properties for elementary symmetric functions we need some results on certain binomial coefficients mod p, where p is prime.

<u>LEMMA 2.2</u>. *(i)* $\binom{\alpha p^\lambda - 1}{p^\lambda} \equiv (\alpha - 1) \bmod p$ *if* $\alpha \ge 2, \lambda \ge 0$.

(ii) *If* $r = p^\lambda$, $n = \alpha p^\lambda - 1$, $\alpha > 1$, $\lambda \ge 0$.

then $\binom{n-k}{r-k} \equiv 0 \bmod p$ *for* $1 \le k < r$.

PROOF. These results may be proved from Lucas' formula for binomial coefficients mod p. We give proofs which are self-contained.

(i) Induction on λ.

If $\lambda = 1$, $\binom{\alpha p^{\lambda}-1}{p^{\lambda}} = \binom{\alpha p - 1}{p} = \dfrac{(\alpha p - 1)\ldots(\alpha p - p)}{1 \ldots p}$

$$\equiv (-1)^{p-1}\left(\frac{\alpha p - p}{p}\right) \bmod p$$

$$\equiv (\alpha - 1) \bmod p.$$

If the result holds for $\lambda = \lambda_0$, then

$$\binom{\alpha p^{\lambda_0+1} - 1}{p^{\lambda_0+1}} = \frac{(\alpha p^{\lambda_0+1} - 1)\ldots(\alpha p^{\lambda_0+1} - p^{\lambda_0+1})}{1 \ldots p^{\lambda_0+1}}$$

$$\equiv \left(\frac{\alpha p^{\lambda_0+1} - p}{p}\right)\left(\frac{\alpha p^{\lambda_0+1} - 2p}{2p}\right)\cdots\left(\frac{\alpha p^{\lambda_0+1} - p^{\lambda_0}p}{p^{\lambda_0}.p}\right) \bmod p$$

$$\equiv \frac{(\alpha p^{\lambda_0} - 1)\ldots(\alpha p^{\lambda_0} - p^{\lambda_0})}{1 \ldots p^{\lambda_0}} \bmod p$$

$$\equiv \binom{\alpha p^{\lambda_0} - 1}{p^{\lambda_0}}$$

$$\equiv (\alpha - 1) \bmod p, \text{ by induction.}$$

(ii) Let $k = p^{\lambda} - t$.

Then $\binom{n-k}{r-k} = \binom{(\alpha - 1)p^{\lambda} + t - 1}{t}$ where $1 \le t < p^{\lambda}$

$$= \frac{[(\alpha - 1)p^{\lambda}][(\alpha - 1)p^{\lambda} + 1]\ldots[(\alpha - 1)p^{\lambda} + t - 1]}{t \qquad 1 \qquad \ldots \qquad (t - 1)}$$

To show that this is zero mod p, we only consider factors divisible by p. These are

$$\frac{[(\alpha - 1)p^{\lambda}][(\alpha - 1)p^{\lambda} + p]\dots[(\alpha - 1)p^{\lambda} + \left[\frac{t-1}{p}\right] p]}{t.p\dots(\left[\frac{t-1}{p}\right] p)}$$

$$= \frac{(\alpha - 1)p^{\lambda}}{t} \begin{pmatrix} (\alpha - 1)p^{\lambda-1} + \left[\frac{t-1}{p}\right] \\ \left[\frac{t-1}{p}\right] \end{pmatrix} \text{ if } (t - 1) \geq p$$

$= 0$ otherwise.

In each case, the result is zero mod p. □

THEOREM 2.12. *If* S_r^n *denotes the elementary symmetric polynomial of degree* r *in* n *variables over* $\mathbb{F}_q$, $q = p^t$, *then* S_r^n *is a permutation polynomial over* $\mathbb{F}_q$ *if*

(i) $r = p^e$, $e \in \mathbb{Z}$

and *(ii)* $n = \alpha r - 1$, *where* $\alpha \in \mathbb{Z}$, $\alpha \not\equiv 1 \bmod p$.

PROOF. By lemma 2.1 it suffices to show that $f(\alpha) = S_r^n(x_1 + \alpha,\dots,x_n + \alpha)$ is a permutation polynomial in α for any choice of $(x_1,\dots,x_n)$. A typical term of $f(\alpha)$ is

$\overbrace{(x_1 + \alpha)\dots(x_n + \alpha)}^{r \text{ terms}}$, where not all x_i occur in each term

$$= \alpha^r + (\overbrace{x_1 + \dots + x_n}^{r \text{ terms}})\alpha^{r-1} + (\overbrace{x_1x_2 + \dots + x_1x_n}^{\binom{r}{2} \text{ terms}})\alpha^{r-2} + \dots + x_1 \dots x_n \quad (*)$$

S_r^n has $\binom{n}{r}$ terms. Consider the coefficient of α^{r-k} in $f(\alpha)$. This is a multiple m of $S_r^n(x_1,\dots,x_n)$. Since the coefficient of α^{r-k}

in $(*)$ has $\binom{r}{k}$ terms, and S_k^n has $\binom{n}{k}$ terms, $m\binom{n}{k} = \binom{r}{k}\binom{n}{r}$, thus $m = \binom{n}{r}\binom{r}{k}/\binom{n}{k}$, and so

$$m = \binom{n-k}{r-k}, \text{ or}$$

$$f(\alpha) = \sum_{k=0}^{r} \binom{n-k}{r-k} S_k^n(x_1,\ldots,x_n)\alpha^{r-k}$$

We show that, under the conditions of the theorem, the coefficient of α^r is non-zero, and the coefficient is α^t is zero for $1 \le t < r$. The coefficient of α^r is $\binom{n}{r} = \binom{\alpha p^e - 1}{p^e} \equiv (\alpha - 1) \bmod p$, and this is non-zero since $\alpha \not\equiv 1 \bmod p$. The coefficient of α^{r-k} is $\binom{n-k}{r-k} = 0$ for $0 < k < r$. Thus $f(\alpha)$ is a permutation polynomial in α and so $S_r^n(x_1,\ldots,x_n)$ is a permutation polynomial. $\square$

<u>COROLLARY</u>. *If* $S_r^n(x_1,\ldots,x_n)$ *is the elementary symmetric polynomial of degree* r *in* n *variables, and* r, n *satisfy the conditions of theorem 2.12, then* S_r^n *is a permutation polynomial over all extension fields of* $\mathbb{F}_p$.

This is in contrast to the single variable case, where the only permutation polynomials having this property are those of the form $ax^{p^j} + b$, $j \in \mathbb{Z}$, $a,b \in \mathbb{F}_p$.

Recalling the definition of ρ in lemma 2.1, we call a polynomial f ρ-constant if the identity $f(x_1 + \alpha, \ldots, x_n + \alpha) = f(x_1,\ldots,x_n)$ holds. Thus, amongst the elementary symmetric functions, S_r^n is ρ-constant over $\mathbb{F}_q$ if $(n - r) \equiv -1 \bmod p^t$, where $p^t > r$, $p^{t-1} \leq r$. The set of all ρ-constant functions (not necessarily in the same variables) is closed under addition and multiplication. If $n = 1$, then a ρ-constant function is a constant function. If $f(x_1,\ldots,x_n)$ permutes each ρ-class (e.g. the S_r^n of theorem 2.12) and $g(y_1,\ldots,y_t)$ is ρ-constant, where $\{x_i\} \cap \{y_j\}$ may be non-empty, then $f + g$ permutes each ρ-class and so is a permutation polynomial. For example, over $\mathbb{F}_3$, S_3^5 is a permutation polynomial , and S_1^3 is a ρ-constant (and a permutation polynomial). Thus $S_3^5(x_1,\ldots,x_5) + \lambda(x_1 + x_2 + x_3)$ is a permutation polynomial over $\mathbb{F}_3$ (and, in fact over all $\mathbb{F}_q$, $q = 3^e$), for $\lambda \not\equiv 0 \bmod 3$. In general, if, over $\mathbb{F}_p$, $f(x_1,\ldots,x_n)$ permutes each ρ-class and $g(x_1,\ldots,x_t)$ is ρ-constant, then $(f + \lambda g)(x_1,\ldots,x_{\max(n,t)})$, $\lambda \neq 0$, is a permutation polynomial over all extension fields of $\mathbb{F}_p$.

CHAPTER 3

ORTHOGONAL SYSTEMS OF POLYNOMIALS OVER A FINITE FIELD WITH COEFFICIENTS IN A SUBFIELD

It was noted in Chapter 2 that any orthogonal system $(f_1,\ldots,f_r)$ in k variables, $r \le k$, may be extended to an orthogonal system $f_1,\ldots,f_k$ (Niederreiter [30]). Suppose now that $f_1,\ldots,f_r$ have coefficients in $\mathbb{F}_q$, and that $(f_1,\ldots,f_r)$ is an orthogonal system over an extension field $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. The question arises whether it is possible to extend $(f_1,\ldots,f_r)$ to an orthogonal system over $\mathbb{F}_{q^n}$, with coefficients in $\mathbb{F}_q$. We answer this question in the affirmative, and calculate the number of ways in which this can be done.

Carlitz and Hayes [4] have investigated the structure of the group $A(q^n)$ of permutations p of $\mathbb{F}_{q^n}$ induced by polynomials with coefficients in $\mathbb{F}_q$. We extend these results to multivariable polynomial vectors. We begin by determining the structure of the group $A^k(q^n)$ of permutations of $\mathbb{F}^k_{q^n}$ induced by permutation polynomial vectors with coefficients in $\mathbb{F}_q$. We then consider the problem outlined in the preceeding paragraph.

1. THE GROUP $A^k(q^n)$

Since the polynomial $(x^{q^n} - x)$ induces the zero map on $\mathbb{F}_{q^n}$, we may suppose that all polynomials have degree less than q^n in each variable.

LEMMA 3.1. $p(x_1,\ldots,x_k) \in \mathbb{F}_{q^n}[x_1,\ldots,x_k]$ *has coefficients in* $\mathbb{F}_q$ *if and only if* $p(a_1^q,\ldots,a_k^q) = [p(a_1,\ldots,a_k)]^q$, *for all* $a_1,\ldots,a_k \in \mathbb{F}_{q^n}$.

PROOF. If $p(x_1,\dots,x_k)$ has coefficients in $\mathbb{F}_q$, the condition is evident from the fact that the Frobenius automorphism $\phi:x \to x^q$ of $\mathbb{F}_{q^n}$ fixes $\mathbb{F}_q$. Conversely, if

$$p = \sum a_{i_1,\dots,i_k} x_1^{i_1} \dots x_k^{i_k} ,$$

where $a_{i_1,\dots,i_k} \in \mathbb{F}_{q^n}$, then

$$[p(x_1,\dots,x_k)]^q - p(x_1^q,\dots,x_k^q) = \sum b_{i_1,\dots,i_k} x_1^{qi_1} \dots x_k^{qi_k} ,$$

where $$b_{i_1,\dots,i_k} = a_{i_1,\dots,i_k}^q - a_{i_1,\dots,i_k} .$$

Since the map $\phi:x \to x^q$ is an automorphism of $\mathbb{F}_{q^n}$, the polynomial

$$\sum b_{i_1,\dots,i_k} x_1^{i_1} \dots x_k^{i_k}$$

induces the zero map on $\mathbb{F}_{q^n}$, and since its degree in each variable is less than q^n, each coefficient is 0. Thus $b_{i_1,\dots,i_k} = 0$, which implies that

$$p \in \mathbb{F}_q[x_1,\dots,x_k] . \quad \square$$

Let $\underline{a} = (a_1,\dots,a_k)$, $a_i \in \mathbb{F}_{q^n}$. A k-tuple $(a_1^{q^s},\dots,a_k^{q^s})$,$s\in\mathbb{Z}$, will be called a conjugate of $\underline{a}$. By the *degree* of $\underline{a}$, we mean $\operatorname{lcm}_{1\le i\le k} (\deg a_i)$.

Clearly $\deg \underline{a}$ divides n. Further, define $K_d^k = \{\underline{a} \in \mathbb{F}_{q^n}^k : \deg \underline{a} = d\}$, and $\phi^s:(x_1,\dots,x_k) \to (x_1^{q^s},\dots,x_k^{q^s})$.

LEMMA 3.2. *If* $\underline{\alpha} \in K_d^k$, *then the orbit of* $\underline{\alpha}$ *under* $A^k(q^n)$ *is* K_d^k.

PROOF. Let $H_d^k = \{(\alpha_1,\ldots,\alpha_k) : \alpha_i \in \mathbb{F}_{q^d}\}$. Then $K_d^k = H_d^k \setminus \bigcup_{\substack{t|d \\ t\neq d}} H_t^k$. Since each H_d^k is mapped into itself by $A^k(q^n)$, it follows that K_d^k is mapped into itself by $A^k(q^n)$. Hence orbit $(\underline{\alpha}) \subseteq K_d^k$. To show the reverse inclusion, we need to find an $f \in A^k(q^n)$ such that if $\underline{\beta} = (\beta_1,\ldots,\beta_k) \in K_d^k$, then $f(\underline{\beta}) = \underline{\alpha}$. Such an f may be defined as follows. If $\underline{\beta} = \underline{\alpha}^{q^s}$, then $f = \phi^s$. Otherwise define

$$f(x) = \begin{cases} \underline{x} \ , & \text{if } \underline{x} \text{ is not a conjugate of } \underline{\alpha} \text{ or } \underline{\beta} \\ \phi^s(\underline{\beta}) \ , & \text{if } \underline{x} = \phi^s(\underline{\alpha}) \\ \phi^s(\underline{\alpha}) \ , & \text{if } \underline{x} = \phi^s(\underline{\beta}) \ . \end{cases}$$

f is a permutation polynomial since $\underline{\alpha},\underline{\beta}$ both have d conjugates. Further $f\phi = \phi f$, and so $f \in A^k(q^n)$. Hence orbit $(\underline{\alpha}) = K_d^k$. □

For each divisor d of n, we denote the group of permutations of K_d^k with $g\phi = \phi g$ by ${}_dG_n^k$. $A^k(q^n)$ may be mapped into ${}_dG_n^k$ by θ_d, where $\theta_d(f) = f|_{K_d^k}$. Thus there is a homomorphism $\theta : A^k(q^n) \to \underset{d|n}{\times} {}_dG_n^k$, from $A^k(q^n)$ to the direct product of the ${}_dG_n^k$.

THEOREM 3.1. *The homomorphism* θ *is an isomorphism.*

PROOF. We define an inverse homomorphism ψ as follows. Given $(f_d)_{d|n}, f_d \in {}_dG_n^k$, $\psi(f_d) := f$, where f is the orthogonal system which induces the same map on $\mathbb{F}^k_{q^n}$ as each f_d. Since f commutes with ϕ, $f \in A^k(q^n)$. $\square$

Let γ_d be the number of conjugacy classes of K^k_d. Then $|K^k_d| = d\gamma_d$. Let C_d be the cyclic group of order d, and S_n the symmetric group on n objects. Define $\pi : S_{\gamma_d} \to \mathrm{Aut}\,(C_d^{\gamma_d})$ by letting S_{γ_d} permute the γ_d-fold product $C_d^{\gamma_d}$.

<u>THEOREM 3.2.</u> ${}_dG^n_k$ *is isomorphic to the semidirect product* $C_d^{\gamma_d} \underset{\pi}{\times} S_{\gamma_d}$.

<u>PROOF.</u> The proof is essentially the same as that of theorem 2 of Carlitz and Hayes [4], with the conjugacy classes of a replaced by the generalized classes of $\underline{\alpha}$, and γ_d replacing $\pi(d)$. $\square$

<u>COROLLARY.</u> *The order of* $A^k(q^n)$ *is* $\prod_{d|n} (\gamma_d!)d^{\gamma_d}$.

It remains only to evaluate γ_d.

<u>THEOREM 3.3.</u> $\gamma_n = \frac{1}{n} \sum_{d|n} q^{dk} \mu(\frac{n}{d})$.

<u>PROOF.</u> $\sum_{d|n} d\gamma_d = q^{nk}$, and so, by the Möbius inversion formula (Lemma 1.6)

$$n\gamma_n = \sum_{d|n} q^{dk} \mu(\tfrac{n}{d}) \ . \ \square$$

2. ORTHOGONAL q-MAPS AND q-SYSTEMS

By lemma 3.1, a permutation polynomial p in k variables over $\mathbb{F}_{q^n}$ has coefficients in $\mathbb{F}_q$ if and only if p commutes with ϕ, the Frobenius automorphism of $\mathbb{F}_{q^n}$. Any such polynomial may be extended to a permutation polynomial vector over $\mathbb{F}_{q^n}$, but this vector will in general not have its coefficients in $\mathbb{F}_q$. We now find necessary and sufficient conditions for a polynomial to be a component of a permutation polynomial vector over $\mathbb{F}_{q^n}$, with coefficients in $\mathbb{F}_q$. We shall call an orthogonal system $(f_1,\ldots,f_r)$ in k variables, over $\mathbb{F}_{q^n}$, $r \le k$, with coefficients in $\mathbb{F}_q$, an orthogonal q-system if it can be extended to an orthogonal system $(f_1,\ldots,f_k)$ with coefficients in $\mathbb{F}_q$. We aim to characterise the maps of $\mathbb{F}_{q^n}$ induced by such systems. To this end we introduce the following definition.

DEFINITION 3.1. A map $\sigma : \mathbb{F}^k_{q^n} \to \mathbb{F}^r_{q^n}$, $r \le k$, is called an *orthogonal* q-map if the two following conditions hold:

(i) if $\sigma(a_1,\ldots,a_k) = (\alpha_1,\ldots,\alpha_r)$ and $\sigma(a_1^q,\ldots,a_k^q) = (\beta_1,\ldots,\beta_r)$, then $\alpha_i^q = \beta_i$, $1 \le i \le r$.

(ii) if $\mathbb{F}_{q^t}$, $t|n$, is a subfield of $\mathbb{F}_{q^n}$, then σ maps $\mathbb{F}^k_{q^t}$ onto $\mathbb{F}^r_{q^t}$, and the equation $\sigma(x_1,\ldots,x_k) = \alpha$ has $q^{t(k-r)}$ solutions for each $\alpha \in \mathbb{F}^r_{q^t}$.

LEMMA 3.3. *Any orthogonal q-map σ may be represented as the map $\mathbb{F}^k_{q^n} \to \mathbb{F}^r_{q^n}$ induced by a polynomial vector with coefficients in $\mathbb{F}_q$.*

PROOF. Any map $\sigma : \mathbb{F}^k_{q^n} \to \mathbb{F}^r_{q^n}$ may be represented as a polynomial vector over $\mathbb{F}_{q^n}$. Condition (i) and lemma 3.1 show that the coefficients of such a vector lie in $\mathbb{F}_q$. □

We denote the set of orthogonal q-maps $\mathbb{F}^k_{q^n} \to \mathbb{F}^r_{q^n}$ by $S(n,k,r,q)$. Then $S(n,k,k,q) = A^k(q^n)$. By section one, there exists an orthogonal system f over $\mathbb{F}_{q^n}$ in k variables with coefficients in $\mathbb{F}_q$, which we call an orthogonal q-system, and so the vector of the first r components of f is an element of $S(n,k,r,q)$, which is therefore non-empty. In Section 1 we regarded $A^k(q^n)$ as a permutation group over $\mathbb{F}^k_{q^n}$. We now consider $A^k(q^n)$ as a permutation group over $S(n,k,r,q)$, $r \leq k$. Where no confusion can arise, we denote $S(n,k,r,q)$ by S_r. If $f \in S_r$ and $\psi \in A^k(q^n)$, define $\psi(f)$ by

$$\psi(f)(u_1,\ldots,u_k) = f(\psi(u_1,\ldots,u_k)) \ .$$

THEOREM 3.4. *The group* $A^k(q^n)$ *acts as a transitive permutation group on* S_r, *where the action of* $A^k(q^n)$ *is defined by* $\psi(f) = f(\psi)$, *with* $f \in S_r$, $\psi \in A^k(q^n)$.

PROOF. We show firstly that if $f \in S_r$, $\psi \in A^k(q^n)$, then $\psi(f) \in S_r$.

$$\begin{aligned}\psi(f)(u_1^q,\ldots,u_k^q) &= f(\psi_1(u_1^q,\ldots,u_k^q),\ldots,\psi_k(u_1^q,\ldots,u_k^q)) \\ &= f([\psi_1(u_1,\ldots,u_k)]^q,\ldots,[\psi_k(u_1,\ldots,u_k)]^q)\end{aligned}$$

where ψ_i is the map of $\mathbb{F}^k_{q^n} \to \mathbb{F}_{q^n}$ formed by taking the i'th projection of ψ. Since

$\psi(f)(u_1,\dots,u_k) = f(\psi_1(u_1,\dots,u_k),\dots,\psi_k(u_1,\dots,u_k))$ and $f \in S_r$, $\psi(f)$ satisfies condition (i) of definition 3.1. Now let $\mathbb{F}_{q^t} \subseteq \mathbb{F}_{q^n}$. Then $\psi(f) : \mathbb{F}^k_{q^t} \to \mathbb{F}^r_{q^t}$. Consider the equation $\psi(f)(x_1,\dots,x_k) = \alpha$, $\alpha \in \mathbb{F}^r_{q^t}$. Since ψ induces a bijection of $\mathbb{F}^k_{q^t}$, the number of solutions of this equation is the same as the number of solutions of $f(x_1,\dots,x_k) = \alpha$ and so $\psi(f) \in S_r$. We now show that ψ induces a permutation of S_r. Suppose $\psi(f_1) = \psi(f_2)$. If $(v_1,\dots,v_k) \in \mathbb{F}^k_{q^n}$, then there exists $(u_1,\dots,u_k) \in \mathbb{F}^k_{q^n}$ such that $\psi(u_1,\dots,u_k) = (v_1,\dots,v_k)$. Then

$$\psi(f_1)(u_1,\dots,u_k) = \psi(f_2)(u_1,\dots,u_k) \Rightarrow f_1(v_1,\dots,v_k) = f_2(v_1,\dots,v_k),$$

and so $f_1 = f_2$. To show that $A^k(q^n)$ acts transitively on S_r, we firstly extend the notation introduced in section 1. $K^s_d = \{\underline{v} \in \mathbb{F}^s_{q^n} : \deg \underline{v} = d\}$, where $\deg(v_1,\dots,v_s) = \operatorname{lcm}\{\deg v_1,\dots,\deg v_s\}$. Then $\mathbb{F}^r_{q^n} = \bigcup_{d|n} K^r_d$. If $t|d$, $d|n$, $f \in S_r$, define

$$\alpha_f(t,d) = \{\underline{x} \in \mathbb{F}^k_{q^n} : \underline{x} \in K^k_d \text{ and } f(\underline{x}) \in K^r_t\} .$$

Then $\mathbb{F}^k_{q^n} = \bigcup_{\substack{d|n \\ t|d}} \alpha_f(t,d)$, if $f \in S_r$. If $f_1, f_2 \in S_r$, we construct $\psi \in A^k(q^n)$ with $\psi(f_2) = f_1$ as follows. Corresponding to f_1, f_2, there are partitions α_{f_1}, α_{f_2}, of $\mathbb{F}^k_{q^n}$. Choose a set R_t of representatives of the conjugacy classes of $\mathbb{F}^t_{q^n}$, for $t = k$ and $t = r$. Since $\alpha_f(t,d)$ is closed under conjugation by (i) of definition 3.1, $\beta_f(t,d) = R_k \cap \alpha_f(t,d)$ is a set of representatives of the conjugacy classes of elements of $\alpha_f(t,d)$. For $y \in R_r \cap K_t^r$ define

$$\gamma(t) = \gamma(f,y,t,d) = f^{-1}(y) \cap \beta_f(t,d) .$$

Then from definition 3.1, the cardinality of $\gamma(f,y,t,d)$ depends only on t and d. Take any bijection from $\gamma(f_1)$ to $\gamma(f_2)$. By preserving conjugates, this extends uniquely to a bijection of $\alpha_{f_1}(t,d)$ to $\alpha_{f_2}(t,d)$ and hence from $\mathbb{F}^k_{q^n}$ to itself. From the construction, this bijection ψ commutes with ϕ^k and so $\psi \in A^k(q^n)$. Further $\psi(f_2) = (f_1)$, and so $A^k(q^n)$ acts transitively on S_r. □

The connection between orthogonal q-maps and orthogonal q-systems is given by

<u>THEOREM 3.5</u>. *A polynomial vector* $f = (f_1,\ldots,f_r)$ *in* k *variables over* $\mathbb{F}_{q^n}$ *is an orthogonal q-system if and only if the mapping which* f *induces on* $\mathbb{F}^k_{q^n}$ *is an orthogonal q-map.*

<u>PROOF</u>. If f is part of an orthogonal system $f^{(k)} = (f_1,\ldots,f_k)$ in $\mathbb{F}_q$, then $f^{(k)}$ commutes with ϕ^k, and so f satisfies condition (1) of definition 3.1. Since $f^{(k)}$ induces a permutation of $\mathbb{F}^k_{q^t}$, $t|n$, f is an orthogonal system over $\mathbb{F}_{q^t}$, and so condition (ii) holds.

Conversely, consider any orthogonal q-map f, and any orthogonal q-system $g = (g_1,\ldots,g_k)$. Let $g^{(r)} = (g_1,\ldots,g_r)$.

Then $g^{(r)}$ induces an orthogonal q-map on $\mathbb{F}^k_{q^n}$. By theorem 3.4, there exists $\psi \in A^k(q^n)$ with $\psi: g^{(r)} \to f$. This gives a representation of f by polynomials over $\mathbb{F}_q$, and as such is part of $\psi(g)$. Thus f is induced by an orthogonal q-system. □

3. EXTENSIONS OF q-SYSTEMS

In section 2 we showed that orthogonal q-maps are precisely those maps of $\mathbb{F}^k_{q^n}$ to $\mathbb{F}^r_{q^n}$ induced by orthogonal q-systems. We now consider the question of extending a given orthogonal q-system on $\mathbb{F}^r_{q^n}$ to one on $\mathbb{F}^t_{q^n}$, $1 \le r \le t \le n$. We use the following results on permutation groups, which may be found in Passmann [35] p. 12. If G is a permutation group on a set A, let $G_a = \{g \in G : ag = a\}$.

LEMMA 3.4. $\{g \in G : ag = b\} = G_a h$, *where* $b \in A$, *and* $h : a \to b$, $h \in G$. *Further if* G *is transitive, then* $[G:G_a] = |A|$.

THEOREM 3.6. *The number of ways of extending an orthogonal q-system* f *over* $\mathbb{F}^r_{q^n}$ *to one over* $\mathbb{F}^s_{q^n}$, $1 \le r \le s \le n$, *is independent of* f.

PROOF. f is extendable to $\psi \in A^k(q^n)$ if and only if $\psi(u) = f$, where $u(x_1,\ldots,x_n) = (x_1,\ldots,x_r)$. In lemma 3.4, take $G = A^k(q^n)$, $A = S_r$, $a = u$, $b = f$. Then the set of all ψ with $\psi(u) = f$ is a coset of G_a, $a = u$, and so the number of ψ which extend f is given by $|A^k(q^n)|/|S_r|$. Any extension of f to $\psi \in A^k(q^n)$ may be obtained by extending it to some $g \in S_s$, and then extending g to ψ. If the number of extensions of f to S_s is $\lambda(r,s)$, then $|G|\lambda(r,s)/|S_s| = |G|/|S_r|$, and so $\lambda(r,s) = |S_s|/|S_r|$, and this is independent of f. $\square$

Thus the extension question is reduced to evaluating $|S_r|$. We introduce some new notation. Define $\pi_{(n,r)}(t) = \frac{1}{n} \sum_{\substack{d|n \\ t|d}} q^{d(k-r)}\mu(\frac{n}{d})$, where the summation is taken over all divisors d of n such that $t|d$. Note that if $t\nmid n$ then $\pi_{(n,r)}(t) = 0$ and the number of conjugacy classes in K_d^r is $\pi_{(d,k-r)}(1)$.

<u>THEOREM 3.7</u>. *The number of ways of extending an orthogonal q-system* f *over* $\mathbb{F}^r_{q^n}$ *to one over* $\mathbb{F}^s_{q^n}$, $1 \le r \le s \le n$, *is given by* $|S_s|/|S_r|$, *where* $|S_r| = \prod_{d|n} [N(d) \prod_{t|d} M(d,t)t^{\pi_{(t,k-r)}(1)}]$, N(d) *is the multinomial coefficient* $(\pi_{(d,0)}(1) : \pi_{(1,k-r)}(1)\ \pi_{(d,r)}(1)\ ,\ldots,\ t\pi_{(t,k-r)}(1)\pi_{(d,r)}(t)\ ,\ldots,\ d\pi_{(d,k-r)}(1)\pi_{(d,r)}(d))$, *where* t *ranges over the divisors of* d, *and*

$$M(d,t) = \frac{(t\pi_{(d,r)}(t)\pi_{(t,k-r)}(1))!}{(t\pi_{(d,r)}(t)!)^{\pi_{(t,k-r)}(1)}}$$

<u>PROOF</u>. To evaluate $|S_r|$ we begin by evaluating $\lambda(n) = \#\{f^{-1}(y) \cap K_n^k$, where f is a q-orthogonal map and $y \in K_t^r\}$. We regard r,t,q and k as fixed, and n as variable. Further, define $\delta(t,n) = \begin{cases} 0 \text{ if } t\nmid n \\ 1 \text{ if } t|n \end{cases}$. Then $\lambda(n)$ is a well defined function from

$\mathbb{Z}^+ \to \mathbb{Z}^+$, and $\lambda(n) = 0$ if $t \nmid n$. $\sum_{d|n} \lambda(d)$ is the total number of elements of $\mathbb{F}^k_{q^n}$ mapped onto $y \in \mathbb{F}^r_{q^n}$ by f, if $t|n$, and 0 if $t \nmid n$. Thus $\sum_{d|n} \lambda(d) = q^{n(k-r)}\delta(t,n)$. By Möbius inversion

$$\lambda(n) = \sum_{d|n} q^{d(k-r)}\delta(t,d)\mu(\tfrac{n}{d})$$

$$= n\pi_{(n,r)}(t) .$$

Thus the total number of elements of K^k_d mapped into K^r_t is $dt\pi_{(d,r)}(t)\pi_{(t,k-r)}(1)$. Furthermore, the action of a q-orthogonal map on a conjugacy class of K^k_d is determined by its action on a single element, and the images of elements of a conjugacy class are themselves conjugate. Select a set of representatives of the conjugacy classes of K^k_d. Then K^r_t, $r \le k$, must receive $t\pi_{(d,r)}(t)\pi_{(t,k-r)}(1)$ such representatives under an element S_r. To construct a q-orthogonal map on K^k_d, firstly distribute the representatives into lots of size $t\pi_{(d,r)}(t)\pi_{(t,k-r)}(1)$. This may be done in N(d) ways, where N(d) is defined in the statement of the theorem.

Now consider the $t\pi_{(d,r)}(t)\pi_{(t,k-r)}(1)$ representatives which are distributed over K^r_t, This distribution may be effected by choosing a set of representatives of conjugacy classes of K^r_t (in $t^{\pi_{(t,k-r)}(1)}$ ways), and distributing the $t\pi_{(d,r)}(t)\pi_{(t,k-r)}(1)$ elements uniformly over the $\pi_{(t,k-1)}(1)$ classes. There are M(d,t) ways of doing this, where M(d,t) is defined in the statement of the theorem. Thus the total number of elements of S_r is given by

$$|S_r| = \prod_{d|n} (N(d) \prod_{t|d} M(d,t)\ t^{\pi(t,k-r)^{(1)}}). \quad \square$$

CHAPTER 4

SOME GENERALISATIONS OF CHEBYSHEV POLYNOMIALS AND THEIR INDUCED GROUP STRUCTURE OVER A FINITE FIELD

If u,b are rational integers then the polynomial $f(z) = z^2 - uz + b$ has roots σ_1,σ_2 in the complex field, such that $u = \sigma_1 + \sigma_2$ and $b = \sigma_1\sigma_2$. The polynomial $g_k(u;b)$ may be defined by requiring $f_k(z) = z^2 - g_k(u;b)z + b^k$ to have roots σ_1^k,σ_2^k. Thus $g_k(u;b) = \sigma_1^k + \sigma_2^k = \sigma_1^k + b^k\sigma_1^{-k}$ and $b^k = \sigma_1^k\sigma_2^k$ and Waring's formula (see Lausch-Nöbauer [19] page 297) allows the expression of $g_k(u;b)$ as a polynomial in u and b. These polynomials $g_k(u;b)$ are known as Dickson polynomials ([19] page 209), the case $b = 1$ being, up to a linear transformation, the classical Chebyshev polynomials of the first kind. The explicit form of such a polynomial is given in definition 2.4. When these polynomials are considered as being defined over a finite field $\mathbb{F}_q$ (i.e. the coefficients are reduced modulo the field characteristic) it eventuates that some of them are permutation polynomials. The necessary and sufficient condition for $g_k(u;b)$ to be a permutation polynomial is that $(k,q^2-1) = 1$, where q is the order of the field (see [19] page 209). Nöbauer [33] showed that the set $\{g_k(u;b),\ b \text{ fixed}\}$ is closed under composition of polynomials if and only if $b = 0$, 1, or -1, and determined the structure of the groups of permutations induced by polynomials of this type in these cases.

Lidl [23] extended this definition to an n-variable form of the Chebyshev polynomials and their algebraic properties were considered by Lidl and Wells [26]. In this formulation the quadratic $f(z)$ is replaced by a polynomial

$$r(u_1,\ldots,u_n,z) = z^{n+1} - u_1z^n + \ldots + (-1)^n u_nz + (-1)^{n+1}b$$
$$= (z - \sigma_1) \ldots (z - \sigma_{n+1}) ,$$

where $u_i \in \mathbb{Z}$, $\sigma_i \in \mathbb{C}$. When taken over $\mathbb{F}_q$, r has (n+1) not necessarily distinct roots in $\mathbb{F}_{q^{(n+1)!}}$.

If k is a positive integer, set

$$r^{(k)}(u_1,\ldots,u_n,z) = (z - \sigma_1^k) \ldots (z - \sigma_{n+1}^k) .$$

The coefficients $g_t^{(k)}(u_1,\ldots,u_n)$ of $r^{(k)}$ are elementary symmetric functions of $\sigma_1^k,\ldots,\sigma_{n+1}^k$, and so are symmetric functions of $\sigma_1,\ldots,\sigma_{n+1}$. Thus the coefficients of $r^{(k)}$ are all polynomials in $(u_1,\ldots,u_n)$ by the fundamental theorem on symmetric functions. In this way we obtain a polynomial vector $g(n,k,b) = (g_1^{(k)}(u_1,\ldots,u_n,b),\ldots,g_n^{(k)}(u_1,\ldots,u_n,b))$. The explicit forms, recurrence relations, and generating functions of these polynomials are contained in [23]. Here we deal only with their algebraic properties. When considered as a polynomial vector over $\mathbb{F}_q$, g(n,k,b) induces a permutation of $(\mathbb{F}_q)^n$ if and only if $(k,q^s - 1) = 1$, $s = 1,\ldots,n + 1$, for $b \neq 0$, $s = 1,\ldots,n$ for $b = 0$ (see [26] page 106). In the two variable case the corresponding group of permutations has been determined by Lidl ([20] and [21]). Here we begin by considering a more general construction. We take

$$\begin{aligned} r(u_1,\ldots,u_n,z) &= z^n - u_1 z^{n-1} + \ldots + (-1)^n u_n \\ &= (z - \sigma_1) \ldots (z - \sigma_n) . \end{aligned}$$

If f(z) is a fixed polynomial, define

$$\begin{aligned} r^{(f)}(u_1,\ldots,u_n,z) &= (z - f(\sigma_1)) \ldots (z - f(\sigma_n)) \\ &= z^n - g_1^{(f)}(u_1,\ldots,u_n)z^{n-1} + \ldots + (-1)^n g_n^{(f)}(u_1,\ldots,u_n). \end{aligned}$$

Then, as before, each $g_n^{(f)}$ may be written as a polynomial in $u_1,\ldots,u_n$. When $f(z) = z^k$, this essentially corresponds to $g(n,k,0)$ as given above. In the first section of this chapter we examine the properties of the polynomials defined in this way. Then we consider the groups of permutations induced by Chebyshev polynomials in n variables over $\mathbb{F}_q$ and determine which of these groups are cyclic. (This generalises the results in [21], [23] and [26] to the n-dimensional case.) The general results are then applied to obtain a result of Brawley, Carlitz and Levine [3] on polynomials which permute the set of n×n matrices over $\mathbb{F}_q$.

1. THE GENERAL CONSTRUCTION

The construction outlined in the introduction to this chapter defines a polynomial vector $(g_1^{(f)},\ldots,g_n^{(f)})$ which induces a map $\mathbb{F}_q^n \to \mathbb{F}_q^n$. It is more convenient to consider this process as an operation on the set of monic polynomials of degree n over $\mathbb{F}_q$, denoted by $P(q,n)$. Thus if $f \in \mathbb{F}_q[x]$ is a fixed polynomial over $\mathbb{F}_q$, define the operator Δ_f: $P(q,n) \to P(q,n)$ as follows: If $h(x) \in P(q,n)$ and $h(x) = \prod_{i=1}^{n} (x - \alpha_i)$, $\alpha_i \in \mathbb{F}_q^{n!}$, is the factorization of $h(x)$ into linear factors in a suitable extension field of $\mathbb{F}_q$ then $\Delta_f h(x) = \Pi(x - f(\alpha_i))$.

Clearly the map induced by $(g_1^{(f)},\ldots,g_n^{(f)})$ on $\mathbb{F}_q^n$ is a permutation if and only if Δ_f induces a permutation on $P(q,n)$. The following properties follow immediately from the definition:

LEMMA 4.1. $\Delta_f(hg) = \Delta_f h\ \Delta_f g$,

LEMMA 4.2. $\Delta_{fog}h = \Delta_f(\Delta_g h)$.

We will need the following three elementary lemmas. For each divisor d of n, put

$$K_d = \{\alpha = \mathbb{F}_{q^n} : \deg \alpha = d \text{ over } \mathbb{F}_q\}.$$

LEMMA 4.3. *$f(x) \in F_q[x]$ is a permutation polynomial over $\mathbb{F}_{q^n}$, $n \in \mathbb{Z}$, if and only if $f(x)$ induces a permutation of K_d, for each $d|n$.*

PROOF. Let $f(x)$ permute $\mathbb{F}_{q^n}$. Then $f(x)$ permutes $\mathbb{F}_q = K_1$. Let r be the smallest integer such that $f(x)$ does not permute K_r, $r|n$. If $\alpha \in K_r$, suppose that $f(\alpha) \notin K_r$. Then $f(\alpha) \in K_{r'}$ for some $r'|r$, $r' \neq r$. Since $f(x)$ permutes $K_{r'}$ there exists $\beta \in K_{r'}$ with $f(\alpha) = f(\beta)$. But $K_r \cap K_{r'} = \phi$, so $\alpha \neq \beta$. The reverse implication is trivial, as $\mathbb{F}_{q^n}$ is the disjoint union of the K_d, $d|n$. □

LEMMA 4.4. *If $f(x) \in \mathbb{F}_q(x)$ and $f(a) = f(b)$ implies that a,b are conjugate over $\mathbb{F}_q$ when $a,b \in \mathbb{F}_{q^n}$, then $f(x)$ induces a permutation of K_r, for $r|n$.*

PROOF. By induction on r.

If $r = 1$, let $f(a) = f(b)$, $a,b \in \mathbb{F}_q$. a,b conjugate implies a equals b. Hence $f(x)$ induces a permutation of $\mathbb{F}_q = K_1$. Now assume the proposition true for $r < k$. If $f(a) \in K_r$, $r < k$, where $a \in K_k$, then since $f(x)$ induces a permutation of K_r, there exists $b \in K_r$, with $f(a) = f(b)$. Thus a and b are conjugate over $\mathbb{F}_q$.

But all conjugates of a lie in K_k and $K_k \cap K_r = \phi$. Thus $f(a) \in K_k$. If $f(a) = f(b)$ with $a \neq b$, $a,b \in K_k$, then a,b conjugate implies $f(a) = f(a^{q^\ell}) = [f(a)]^{q^\ell}$, $\ell < k$. Thus $f(a) \in \mathbb{F}_{q^\ell}$ and so $f(a) \in K_{\ell'}$, $\ell' < k$, and we have already shown that $f(a) \in K_k$, a contradiction. □

LEMMA 4.5. *Let* $f(x) \in \mathbb{F}_q[x]$. *The following conditions are equivalent.*

(i) $f(a) = f(b)$, $a,b \in \mathbb{F}_{q^n}$, *implies* a,b *are conjugate over* $\mathbb{F}_q$.

(ii) *If* $a,b \in \mathbb{F}_{q^n}$, *and* $f(a)$, $f(b)$ *are conjugate over* $\mathbb{F}_q$, *then* a,b *are conjugate over* $\mathbb{F}_q$.

(iii) $f(x)$ *is a permutation polynomial over* $\mathbb{F}_{q^n}$.

PROOF. (ii) → (i) and (iii) → (i) are trivial.

(i) → (ii) Let $f(a)$, $f(b)$ be conjugate over $\mathbb{F}_q$. Then $f(b) = [f(a)]^{q^k} = f(a^{q^k})$, $k < n$. Thus b and a^{q^k} are conjugate over $\mathbb{F}_q$ and so a and b are conjugate over $\mathbb{F}_q$.

(i) → (iii) by Lemmas 4.3 and 4.4. □

We are now in a position to prove our main result.

THEOREM 4.1. Δ_f *induces a permutation of* $P(q,n)$ *if and only if* $f(x)$ *is a permutation polynomial over* $\mathbb{F}_{q^r}$, *for each* $r \leq n$.

PROOF. (i) Sufficiency

We note that if $h(x)$ is irreducible of degree $r \leq n$ then $\Delta_f h$ is irreducible, for if $h = \prod_0^{r-1} (x - \sigma^{q^j})$, $\sigma \in \mathbb{F}_{q^r}$, then $\Delta_f h$ has as conjugates over $\mathbb{F}_q$ of $f(\sigma)$, and these are all distinct since f is a permutation polynomial over $\mathbb{F}_{q^r}$.

If $h = \Pi f_i$,$g=\Pi g_j$ are the factorizations of h and g into products of irreducibles over $\mathbb{F}_q$, and if $\Delta_f h = \Delta_f g$, then $\Pi\Delta_f h_i$, $\Pi\Delta_f g_j$ are factorizations of $\Delta_f h$ into a product of irreducibles over $\mathbb{F}_q$, and so for each i there is a j with $\Delta_f h_i = \Delta_f g_j$, degree h_i= degree $g_j = r$. If h_i has roots σ^{q^s}, and g_j has roots τ^{q^t}, then $f(\sigma) = f(\tau^{q^k})$, for some $k < n$. Since f(x) is a permutation polynomial over $\mathbb{F}_{q^r}$, $\sigma = \tau^{q^k}$. Thus the conjugates of σ and τ coincide and $f_i = g_j$. Hence h = g.

(ii) <u>Necessity</u>.

If f(x) is not a permutation polynomial over $\mathbb{F}_{q^r}$, then by Lemma 4.5 there exist non-conjugate $\sigma,\tau \in \mathbb{F}_{q^r}$ with $p(\sigma) = p(\tau)$. The field polynomials of σ and τ , h_1, h_2 respectively, are distinct of degree r, but $\Delta_f h_1 = \Delta_f h_2$. Let $g_1(x) = x^{n-r}h_1, g_2 = x^{n-r}h_2$. Then $g_1(x) \neq g_2(x)$ but $\Delta_f g_1 = \Delta_f g_2$, and degree g_1 = degree g_2 = n.

<u>Lemma</u> 4.6 Let $\lambda(x) = \text{LCM}\ (x^q - x,\ldots,x^{q^n} - x)$.If $f(x) \equiv r(x) \bmod \lambda(x)$ then $\Delta_f h = \Delta_r h$, for all $h(x) \in P(q,r)$, $k \leq n$.

<u>Proof</u>. If $f(x) \equiv r(x) \bmod \lambda(x)$ then $p(x) \equiv r(x) \bmod (x^{q^k} - x)$, for $k \leq n$. Any root σ of h(x) lies in $\mathbb{F}_{q^k}$ for some $k \leq n$, and so $f(\sigma) = r(\sigma)$. Thus $\Delta_f h = \Delta_r h$.

<u>Lemma</u> 4.7 The set G_n of polynomials $f(x) \in \mathbb{F}_q[x]$ such that

(i) degree $f(x) <$ degree $\lambda(x)$

(ii) $f(x)$ *induces a permutation of* $\mathbb{F}_{q^k}$*, for each* $k \le n$*, forms a group under composition mod* $\lambda(x)$.

PROOF. If $f(x) * r(x)$ is defined to be $(f \circ r)(x) = f(r(x)) \bmod \lambda(x)$ then $f \circ r - f * r = t\lambda$, for some $t \in \mathbb{F}_q[x]$. Since $\lambda(\sigma) = 0$ if $\sigma \in \mathbb{F}_{q^k}$, $(f \circ r)(\sigma) = (f * r)\sigma$. But $f \circ r$ induces a permutation of $\mathbb{F}_{q^k}$, and thus so does $f * r$. The identity of G_n is x and inverses exist since that system is finite and cancellative. □

We now proceed to determine the group P_n of permutations of $P(q,n)$ induced by this process. By Lemma 4.6 it is sufficient to consider the action of Δ_f for $f \in G_n$.

The structure of G_n was determined by Carlitz and Hayes [4]. We now investigate the structure of P_n.

LEMMA 4.8. *The map* $\theta\colon f \to \Delta_f$ *is a homomorphism from* G_n *onto* P_n.

PROOF. By Lemmas 4.2 and 4.7 and Theorem 4.1. □

LEMMA 4.9. *Ker* $\theta = \{f \in G_n\colon f(\sigma)$ *is a conjugate of* σ*, for all* $\sigma \in \mathbb{F}_{q^k}$, $k \le n.\}$

PROOF. If $\theta(f)$ induces the identity map on $P(q,n)$ then $\Delta_f h = h$, for all h of degree $\le n$. Let $\sigma \in \mathbb{F}_{q^k}$, and h be the minimal polynomial of σ. Then $\Delta_f h = h$ implies $f(\sigma)$ is a conjugate of σ. Conversely, if $h \in P(q,n)$, then $h = \prod h_i$, where the h_i are irreducible over $\mathbb{F}_q$. h_i has roots $\sigma,\ldots,\sigma^{q^{k-1}}$, $k = \deg h_i$, and so $f(\sigma)$

is a conjugate of σ. Since $f(\sigma^{q^\ell}) = [f(\sigma)]^{q^\ell}$, $f(\sigma^{q^\ell})$ runs through the set $\{\sigma^{q^m}\}$. Hence $\Delta_f h_i = h_i$, and $\Delta_f h = h$. □

We denote by A_d the group of permutations of K_d which induce permutations on the set of equivalence classes of conjugate elements.

<u>LEMMA 4.10</u>. *If* $f \in G_n$, *then* f *induces a permutation of* K_d, *for each* $d \leq n$. *Denote this permutation by* p_d. *Define* $\psi: G_n \to A_1 \times A_2 \times \ldots \times A_n$ *by*

$$\psi: p \to (p_1,\ldots,p_n) \ .$$

Then ψ *is a group isomorphism.*

<u>PROOF</u>. To show that ψ is surjective, let $\pi_1,\ldots,\pi_n$ be arbitrary elements of $A_1,\ldots,A_n$. Consider $\mathbb{F}_{q^{n!}}$. Choose on each K_d, $n < d \leq n!$, any permutation π_d of K_d which induces a permutation on the conjugacy classes in K_d. Now consider the map π which is π_i on each K_i, $1 \leq i \leq n!$. Since π commutes with the Frobenius automorphism of $\mathbb{F}_{q^{n!}}$, there is a polynomial $f(x)$ of degree less than $q^{n!}$ with coefficients in $\mathbb{F}_q$ which induces π on $\mathbb{F}_{q^{n!}}$. The reduction of $f(x)$ mod $\lambda(x)$ induces π_i on each A_i, since each $\mathbb{F}_{q^i}$ is a subfield of $\mathbb{F}_{q^{n!}}$, and so $f(x) \in G_n$. If $f \in \operatorname{Ker} \psi$, then $f(x)$ induces the identity on K_d for all $d \leq n$. Hence $f(x) \equiv x \bmod (x^{q^d} - x)$ for all $d \leq n.$, and so $f(x) \equiv x \bmod \lambda(x)$. The other properties of ψ are obvious. □

Each $\pi \in A_i$ induces a permutation of the set of conjugacy classes of K_d. If there are $\pi(d)$ classes in K_d then this gives rise to a homomorphism from A_d to $S_{\pi(d)}$, the symmetric group on $\pi(d)$ elements. Thus there is a homomorphism $\phi: A_1 \times \ldots \times A_n \to S_{\pi(1)} \times \ldots \times S_{\pi(n)}$. Define $\mu = \phi \circ \psi: G_n \to S_{\pi(1)} \times \ldots \times S_{\pi(n)}$.

LEMMA 4.11. *Ker* μ = *Ker* θ.

PROOF. If $f \in \operatorname{Ker} \mu$, then f induces the identity map on the set of conjugacy classes of K_d, $d \le n$. This means that $f(\sigma)$ is a conjugate of σ, for all $\sigma \in \mathbb{F}_{q^k}$, $k \le n$. Thus $f \in \operatorname{Ker} \theta$. Conversely, if $f \in \operatorname{Ker} \theta$, then $\psi(f)$ induces the identity on the set of conjugacy classes and so $f \in \operatorname{Ker} \mu$. □

THEOREM 4.12. *The group* P_n *of maps of* $P(q,n) \to P(q,n)$ *induced by elements of* G_n *is isomorphic to the product of* n *symmetric groups of orders* $\pi(k)$, $k \le n$, *where*

$$\pi(k) = k^{-1} \sum_{d|k} \mu(\tfrac{k}{d}) q^d, \text{ where } \mu \text{ is the Möbius } \mu\text{-function.}$$

PROOF. From Lemmas 4.8 and 4.11. The number of conjugacy classes in K_k is the number of monic irreducible polynomials of degree k in $\mathbb{F}_q[x]$, given by $\pi(k)$ above (lemma 1.7). □

2. CHEBYSHEV POLYNOMIALS IN SEVERAL VARIABLES

As stated in section 1, the Chebyshev polynomial vector $g(n,k,b)$ is a permutation polynomial vector if and only if $(k,q^r - 1) = 1$, $1 \le r \le n$, for $b = 0$, and $(k,q^r - 1) = 1$, $1 \le r \le n + 1$, for $b \ne 0$. The case $b = 0$ in fact follows directly from Theorem 4.1, as the polynomial x^k is a permutation polynomial over $\mathbb{F}_q$ if and only if $(k,q-1) = 1$. It was shown by Lidl and Wells [26] that the set $\{g(n,k,b)\}$, for b fixed, is closed under composition if and only if $b = 0,1$, or -1, and for $n = 2$ the structure of the group of permutations induced by the $g(n,k,b)$ was determined in [20] and [21]. We now extend this to arbitrary n. The case $b = 0$ is treated first, then $b = 1$ and -1 are dealt with together.

The case $b = 0$.

THEOREM 4.3. *The group* G *of mappings of* $\mathbb{F}_q^n \to \mathbb{F}_q^n$ *induced by the permutation polynomial vectors among the vectors* $g(n,k,0)$, *is isomorphic to the group* R *of reduced residues* mod $N = \mathrm{LCM}(q-1, \ldots, q^n - 1)$ *factored by the cyclic subgroup* C *of order* $\mathrm{LCM}(1,\ldots,n)$, generated by q.

PROOF. If $k \equiv k' \bmod N$, then $k \equiv k' \bmod (q^r - 1)$, $1 \le r \le n$, and so the maps $f_k\colon x \to x^k$, $f_{k'}\colon x \to x^{k'}$ coincide on $\mathbb{F}_{q^r}$, $1 \le r \le n$, and so the maps Δ_{f_k}, $\Delta_{f_{k'}}$ are identical on $P(q,n)$. Thus the map $g(n,k,0) \to k'$, where k' is the residue of k mod N, is a homomorphism of the semigroup of permutation vectors amongst the $g(n,k,0)$ onto R. The map ϕ which sends k to the map which $g(n,k,0)$ induces on $\mathbb{F}_q^n$ is then a homomorphism of R onto G. It remains to determine the kernel of this homomorphism. Suppose $k \equiv q^t \bmod N$.

If $f(x) = \Pi f_i(x)$ is the decomposition of $f(x)$ into irreducible factors over $\mathbb{F}_q$, and $f_i(x) = \prod_{r=0}^{n-1} (x - \sigma^{q^r})$ is the factorization of f_i (where f_i has degree n), over its splitting field, then

$$\Delta_{x^k} f_i(x) = \prod_{r=0}^{n-1} (x - \sigma^{q^{r+\tau}}) = f_i(x). \quad \text{Thus } \Delta_{x^k} f = f.$$

Now suppose $k \in \operatorname{Ker} \phi$. Then σ^k is a conjugate of σ for all $\sigma \in \mathbb{F}_{q^r}$, $1 \le r \le n$, by Lemma 4.9. If σ is a primitive element of $\mathbb{F}_{q^r}$, then $\sigma^k = \sigma^{q^\ell}$, since $0 \le \ell \le r$.

Thus $k \equiv q^\ell \bmod (q^r - 1)$ and k is a solution of the system of congruences

$$(1) \qquad \begin{array}{ll} k \equiv 1 & (q - 1) \\ k \equiv 1, q & (q^2 - 1) \\ \vdots & \vdots \\ k \equiv 1, q, \ldots, q^{n-2} & (q^{n-1} - 1) \\ k \equiv 1, q, \ldots, q^{n-1} & (q^n - 1) \end{array}$$

We now show that this system is equivalent to the single condition

(2) $\qquad k \equiv 1, q, \ldots, q^t \bmod N$, where $t = \operatorname{LCM}(1, \ldots, n)$.

Firstly it is clear that any solution to (2) is also a solution to (1). We now wish to determine the order m of $q \bmod N$. If $s = \operatorname{LCM}(1, \ldots, n)$, then $q^s \equiv 1 \bmod N$, since $(q^t - 1) | (q^s - 1)$ for all t with $1 \le t \le n$. Thus $m | s$. Since $q^m \equiv 1 \bmod N$, $N | (q^m - 1)$, and so $(q^t - 1) | (q^m - 1)$, $1 \le t \le n$. This holds only if $t | m$. Thus $s | m$, and so $s = m$, implying that the number of solutions of (2) is $s = \operatorname{LCM}(1, \ldots, n)$. We next show that the number of solutions of (1) is also s, thus proving that every solution of (1) is a solution of (2). We do this by induction on n. When $n = 1$ there is nothing to prove, as $N = q - 1$. By the induction hypothesis, the number of solutions of the first $(n - 1)$ congruences is

$\mathrm{LCM}(1,\ldots,n-1)$, and by the earlier arguments this system is equivalent to $k \equiv 1, q, \ldots, q^{\mathrm{LCM}(1,\ldots,n-1)} \bmod \mathrm{LCM}(q-1,\ldots,q^{n-1}-1)$. Let $N' = \mathrm{LCM}(q-1,\ldots,q^{n-1}-1)$. Suppose $k \equiv q^t \bmod N'$, $k \equiv q^s \bmod (q^n - 1)$. Then $k = q^t + \alpha N' \equiv q^s \bmod (q^n - 1)$, for some $\alpha \in \mathbb{Z}$. $\alpha N' = q^t\,(q^{s-t} - 1) \bmod (q^n - 1)$, where $(s - t)$ is taken mod n. This has a solution if and only if $\gcd(N', q^n - 1) \mid q^t(q^{s-t} - 1)$. Now suppose that n is not of the form p^α, p a prime. Then $n = \prod_{i=1}^{m} p_i^{\alpha_i}$, $m \geq 2$, and $p_i^{\alpha_i} < n$. Thus $k \equiv q^t \bmod N' \rightarrow k \equiv q^t \bmod (q^{p_i^{\alpha_i}} - 1)$ and so $(q^{p_i^{\alpha_i}} - 1) \mid (q^{s-t} - 1)$ for each $p_i^{\alpha_i}$.

Thus $s \equiv t \bmod p_i^{\alpha_i}$, and so $s \equiv t \bmod n$. Hence the choice of s is already determined and so the number of solutions remains the same, namely $\mathrm{LCM}(1,\ldots,n-1) = \mathrm{LCM}(1,\ldots,n)$. If $n = p$, then the condition for a solution is $(q - 1) \mid (q^{s-t} - 1)$, which always holds, and so s is arbitrary, and for each choice of s there is a unique solution mod $\mathrm{LCM}(N', q^n - 1) = N$. Thus the number of solutions is $n\,\mathrm{LCM}(1,\ldots,n-1) = \mathrm{LCM}(1,\ldots,n)$. Now suppose $n = p^\alpha$, $\alpha > 1$. The condition reduces to $s \equiv t \bmod p^{\alpha-1}$, which has p solutions modulo p^α, each giving a unique solution mod N. Thus the number of solutions is $p\,\mathrm{LCM}(1,\ldots,n-1) = \mathrm{LCM}(1,\ldots,n)$. □

<u>The cases b = 1 or -1.</u>

In this section, let $f(x) = x^k$ and let $b = 1$ for characteristic 2, otherwise k odd, $b = \pm 1$. We use the notation of sections 1 and 2.

LEMMA 4.12. *If Δ_f induces the identity map on the set P_b^n of polynomials of degree* n *with constant term* $(-1)^n b$, *then* f *induces the identity map on* $\mathbb{F}_q$, *and* Δ_f *induces the identity map on all polynomials of degree less than* n, *for* $n > 2$.

PROOF. Let ω be a primitive element of $\mathbb{F}_q$ and let

$$h(x) = (x - 1)^{n-3}(x - \omega)^2(x - \omega^{-2}),\ b = 1;$$
$$h(x) = (x - 1)^{n-3}(x - \omega)^2(x + \omega^{-2}),\ b = -1.$$

Then
$$\Delta_f h = (x - 1)^{n-3}(x - \omega^k)^2(x - \omega^{-2k}),\ b = 1;$$
$$\Delta_f h = (x - 1)^{n-3}(x - \omega^k)^2(x + \omega^{-2k}),\ b = -1,$$

since k is assumed to be odd. If the characteristic is 2, consider only the case $b = 1$.

In each case, $h \in P_b^n$, and so $\Delta_f h = h$ by hypothesis. Thus $\omega = \omega^k$, by unique factorization, and ω primitive implied $k \equiv 1\ (q - 1)$. Hence f(x) induces the identity map on $\mathbb{F}_q$. (Note that if $n = 2$, $\omega = \omega^{-k}$ is also possible, and we can only deduce $k \equiv \pm 1\ (q - 1)$). Now let $g(x) \in \mathbb{F}_q[x]$, with degree $g(x) = m < n$. Let g(x) have constant term β. Clearly we may assume $\beta \neq 0$. Define

$h(x) = (x - \frac{(-1)^m b}{\beta})(x - 1)^{n-m-1}g(x)$. h(x) has degree n, and has constant term $(-1)^n b$, and so $\Delta_f h = h$. But

$\Delta_f h = (x - \frac{(-1)^m b}{\beta})(x - 1)^{n-m-1}\Delta_f g$, since $\beta \in \mathbb{F}_q$, and $\beta^k = \beta$. Thus $\Delta_f g = g$. □

LEMMA 4.13. *Let ω be a primitive element of $\mathbb{F}_{q^n}$, and put* $\lambda = \omega^{q-1}$, q *even or odd*, $\mu = \omega^{\frac{1}{2}(q-1)}$, q *odd. Then* $\lambda, \mu \in K_n$.

PROOF. λ has order $\frac{q^n - 1}{q - 1}$. If $\lambda \in \mathbb{F}_{q^r}$, $r < n$, then ord $\lambda \leq q^r - 1$. But $\frac{q^n - 1}{q - 1} > q^r - 1$, $r < n$, and so $\lambda \in K_n$. If $\mu \in \mathbb{F}_{q^r}$, $r < n$, then $\lambda = \mu^2 \in \mathbb{F}_{q^r}$. Since $K_n \cap \mathbb{F}_{q^r} = \phi$, this is impossible. □

THEOREM 4.4. *Δ_f induces the identity map on P_b^{n+1}, $b = \pm 1$ if and only if k satisfies the system*

$$
(3) \qquad
\begin{array}{lll}
k \equiv 1 & (q - 1) & \\
\vdots & \vdots & \\
k \equiv 1, q, \ldots, q^{n-1} & (q^n - 1) & \\
k \equiv 1, q, \ldots, q^n & \frac{q^{n+1} - 1}{q - 1} & \text{in case } b = 1 \\
\text{or} \quad k \equiv 1, q, \ldots, q^n & 2\left(\frac{q^{n+1} - 1}{q - 1}\right) & \text{in case } b = -1.
\end{array}
$$

PROOF. Assume firstly that k satisfies the system. Then if $g(x)$ is irreducible over $\mathbb{F}_q$, and degree $g(x) \leq n$, $\Delta_f g = g$. If g is irreducible of degree $(n + 1)$ and has constant term $(-1)^{n+1}b$, then

$$g(x) = (x - \sigma) \ldots (x - \sigma^{q^n}), \sigma \in \mathbb{F}_{q^{n+1}}$$

where
$$(-1)^{n+1} \sigma^{1+q+\ldots+q^n} = (-1)^{n+1}b ,$$

or
$$\sigma^{(q^{n+1} - 1)/(q - 1)} = b .$$

In the case $b = 1$, this implies that

$$\sigma^k = \sigma^{q^t} \text{ for some } 1 \leq t \leq n ,$$

and so
$$\Delta_f g = g .$$

If $b = -1$, then $\sigma^{(q^{n+1}-1)/(q-1)} = -1$, and $\sigma^{2(q^{n+1}-1)/(q-1)} = 1$, and (3) again gives $\Delta_f g = g$.

Conversely, if $\Delta_f g = g$ for all $g \in P_b^{n+1}$, then by Lemma 4.12, Δ_f induces the identity map on all polynomials of degree $\le n$. Hence k satisfies the first n equations of the system, as in the case $b = 0$.

Now let ω be a primitive element of $\mathbb{F}_{q^{n+1}}$, and take $\lambda = \omega^{q-1}$, $\mu = \omega^{\frac{1}{2}(q-1)}$ for q odd. If q is even consider just the first case, since $1 = -1$. By Lemma 4.13, $\lambda,\mu \in K_n$, and so their minimal polynomials h,g respectively, have degree $(n + 1)$.

The constant terms of h,g are

$$\lambda^{(q^{n+1}-1)/(q-1)} \text{ and } \mu^{(q^{n+1}-1)/(q-1)} ,$$

which equal 1 and -1 respectively.

In the case $b = 1$, it follows that $\Delta_f h = h$ and so

$$\lambda^k = \lambda^{q^t}, \ 0 \le t \le n .$$

Then
$$\omega^{(q-1)k} = \omega^{(q-1)q^t}$$
$$(q - 1)k \equiv (q - 1)q^t \bmod (q^{n+1} - 1)$$
$$k \equiv q^t \bmod \left(\frac{q^{n+1} - 1}{q - 1}\right) .$$

In the case $b = -1$, $\Delta_f g = g$ implies

$$\mu^k = \mu^{q^t}, \ 0 \le t \le n .$$

Then $\omega^{\frac{1}{2}(q-1)k} = \omega^{\frac{1}{2}(q-1)q^t}$

$$\tfrac{1}{2}(q - 1)k \equiv \tfrac{1}{2}(q - 1)q^t \bmod (q^{n+1} - 1)$$

$$k \equiv q^t \bmod 2(q^{n+1} - 1)/(q - 1)\ . \quad \square$$

COROLLARY. *The group* G *of mappings* $\mathbb{F}_q^n \to \mathbb{F}_q^n$ *induced by permutation polynomial vectors* $g(n,k,b)$, *where* $b = 1$ [*resp.* $b = -1$], *is isomorphic to the group of reduced residues*

mod $\mathrm{LCM}(q - 1,\ldots,q^n - 1, \frac{q^{n+1} - 1}{q - 1})$ [*resp.* mod $\mathrm{LCM}(q - 1,\ldots,q^n - 1, 2(q^{n+1} - 1)/(q - 1))$] *factored by the cyclic subgroup generated by* q *of order* $\mathrm{LCM}(1,\ldots,n + 1)$.

PROOF. The proof is essentially the same as for Theorem 4.3, with the following modification. We treat the case $b = 1$, the case $b = -1$ is similar. Let $N = \mathrm{LCM}(q - 1,\ldots,q^n - 1, \frac{q^{n+1} - 1}{q - 1})$. We note firstly that the order of q mod $(\frac{q^{n+1} - 1}{q - 1})$ is $(n + 1)$, since clearly $q^{n+1} \equiv 1 \bmod \frac{q^{n+1} - 1}{q - 1}$, and if q has order $t|(n + 1)$, then $(q^{n+1} - 1)|(q^t - 1)(q - 1)$.

But $\qquad (q - 1)(q^t - 1) = (q^{t+1} - 1) - (q^t + q - 2)\ .$

Since $q \geq 2$, and as $n + 1 \geq 2$, $t \leq \frac{n+1}{2} \leq n$, and so

$$(q^{n+1} - 1) > (q - 1)(q^t - 1), \text{ a contradiction.}$$

We now determine the order of q mod N. Let $s = \mathrm{LCM}(1,\ldots,n + 1)$. Then $q^s \equiv 1 \bmod N$. If $q^m \equiv 1 \bmod N$, then $t|m$, $1 \leq t \leq n$. To show $(n + 1)|m$, we have

$$\left(\frac{q^{n+1} - 1}{q - 1}\right) \mid (q^m - 1) .$$

Let $\gamma = \gcd\,(q^{n+1} - 1, q^m - 1) = q^{\gcd(n+1,m)} - 1$.

Then $$\frac{q^{n+1} - 1}{\gamma} \mid (q - 1)\frac{q^m - 1}{\gamma} .$$

Thus $$\frac{q^{n+1} - 1}{\gamma} \mid (q - 1) ,$$

or $$(q^{n+1} - 1) \mid (q - 1)(q^{\gcd(n+1,m)} - 1) .$$

As before, this is impossible unless $n + 1 = \gcd\,(n + 1,m)$ i.e. $(n + 1)|m$. Now suppose $k \equiv q^t \bmod N'$, $N' = \mathrm{LCM}(q - 1,\ldots,q^n - 1)$, $k \equiv q^s \bmod \left(\frac{q^{n+1} - 1}{q - 1}\right)$. Then

$$k = q^t + \alpha N' \equiv q^s \bmod \left(\frac{q^{n+1} - 1}{q - 1}\right) ,$$

hence $$\alpha N' = q^t(q^{s-t} - 1)\left(\frac{q^{n+1} - 1}{q - 1}\right) .$$

Thus $$\left(\frac{q^m - 1}{q - 1}\right) \mid (q^{s-t} - 1), \text{ for } m|n + 1 .$$

As before this implies $m|(s - t)$, or $s \equiv t \bmod (m)$. The rest of the proof goes through as before, noting that we already know the nature and number of the solutions to the first n congruences. □

Lidl and Müller [25] examined the question of when the group induced by the permutation polynomial vectors $g(n,k,b)$ is cyclic for $n = 2$. The case $n = 1$ was settled earlier by Hule and Müller [17]. We now extend this to the general case.

<u>THEOREM 4.5</u>. *The group* G *induced by the permutation polynomial vectors amongst the* g(n,k,b) *is cyclic if* $q = 2$, $n = 2$ *and* $b = 1$, *or if* $q = 2$ *or* 3, $n = 2$ *and* $b = 0$. G *is not cyclic if* $n > 2$.

<u>PROOF</u>. The fact that G is cyclic in the cases given was established in [25]. The following argument was suggested, in the case $n = 2$, by W. Narkiewicz. If an Abelian group A contains a subgroup isomorphic to the direct sum of three or more copies of C_2, then, when A is factored by a cyclic group, the resulting group cannot be cyclic. If N is the appropriate modulus, $(\mathrm{LCM}(q = 1,\ldots,q^n - 1)$ for $b = 0$, etc.), and q is odd then $8|(q^2 - 1)$, and $(q^3 - 1)$(resp $(\frac{q^3 - 1}{q - 1})$) is divisible by an odd prime. Thus the prime decomposition of N is of the form $N = 2^\beta p_1^{\alpha_1}\ldots p_n^{\alpha_n}$, $p_i \neq 2$, $\beta \geq 3$, $\alpha_i \geq 1$. The group G of reduced residues mod N is isomorphic to the direct sum of the groups $\mathbb{Z}/(2^\beta), \mathbb{Z}/(p_i^{\alpha_i})$. $\mathbb{Z}/(2^\beta) \simeq C_2 \oplus C_{2^{\beta-1}}$, where C_i denotes a cyclic group of order i.

$$\mathbb{Z}/(p_1^{\alpha_1}) \simeq C_{p_1^{\alpha_1-1}} \oplus C_{p_1-1} .$$

Thus G contains a subgroup isomorphic to C_2^3.

If q is even, $q \neq 2$, then $\gcd(q^2 - 1,q^3 - 1) = (q - 1)$, and so there are prime factors of $(q^2 - 1)$ not dividing $(q^3 - 1)$. If $q - 1, q^2 + q + 1$ have a common prime factor k, then $q \equiv 1 \bmod (k)$, and so $q^2 + q + 1 \equiv 3 \bmod k$. Thus unless 3 is the only prime dividing $(q - 1)$, there is a prime dividing $q - 1$ and not

$(q^2 + q + 1)$. If $q - 1 = 3^t$, then

$$q^2 + q + 1 = (q - 1)^2 + 3(q - 1) + 3 = 3\ [3^{2t-1} + 3^t + 1]$$

and the second factor is not divisible by 3. Thus there are at least three odd primes dividing N, and so G contains C_2^3. If $q = 2$, $n \geq 3$, $N = \gcd(1,3,7,15,\ldots)$ and so N is divisible by at least three odd primes as before. □

3. MATRIX PERMUTATION POLYNOMIALS

Brawley, Carlitz, and Levine [3] have determined the polynomials $f(x) \in \mathbb{F}_q[x]$ which permute the set of $n \times n$ matrices over $\mathbb{F}_q$ under substitution. In this section we give a different proof of their result using Theorem 4.1.

THEOREM 4.6. *(Brawley, Carlitz and Levine). Let* $f(x) \in \mathbb{F}_q[x]$. *Then* $f(x)$ *is a permutation polynomial on* $F_{n\times n}$, *the set of* $n \times n$ *matrices with entries in* $\mathbb{F}_q$ *if and only if*

(i) $f(x)$ *is a permutation polynomial over* $\mathbb{F}_{q^r}$, $1 \leq r \leq n$.

and *(ii)* $f'(x)$ *does not vanish on any of the fields*

$$\mathbb{F}_q,\ldots,\mathbb{F}_{q^{[n/2]}}.$$

We first prove the following Lemma.

LEMMA 4.14. $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial on $F_{n\times n}$ if and only if $f(x)$ permutes the similarity classes of $F_{n\times n}$, where the similarity class of $B \in F_{n\times n}$ is $C_B = \{A^{-1}BA \mid A \in F_{n\times n}, A$ invertible$\}$.

PROOF. Suppose $f(x)$ is a permutation polynomial on $F_{n\times n}$. Then f acts on the similarity classes, by defining

$$f(C_B) = C_{f(B)} \cdot$$

If $Y \in C_B$, then $Y = A^{-1}BA$, and $f(Y) = A^{-1} f(B)A \in C_{f(B)}$. The map $C_B \to C_{f(B)}$ is surjective on the set of similarity classes, as otherwise there would be a class with no preimage, and any matrix Y in this class would have no preimage under f, contradicting the fact that f is a permutation polynomial on $F_{n\times n}$. Thus f permutes the similarity classes, as there are a finite number of them.

Now suppose f permutes the similarity classes in $F_{n\times n}$. Then since $|C_{f(B)}| \leq |C_B|$ for all $B \in F_{n\times n}$, each C_B can only be mapped to a class whose order is less than or equal to that of C_B. If $|C_B| = |C_{f(B)}|$ then f induces a one-to-one map of C_B onto $C_{f(B)}$. Thus f can fail to permute $F_{n\times n}$ only if $|C_B| > |C_{f(B)}|$ for some C_B. Let M be the set of classes which are of maximal order n with respect to this property.

Then since all the classes of order greater than n are mapped onto classes of their own cardinality, the set of preimages of the classes of M must be M itself.

Thus $f(x)$ preserves the cardinality of the classes of M, a contradiction. Thus $f(x)$ preserves the cardinality of all classes and so is a permutation polynomial over $F_{n\times n}$. □

PROOF OF THEOREM. Suppose $f(x)$ permutes $F_{n\times n}$. Let $A(x) \in \mathbb{F}_q[x]$, and let C_A be its companion matrix. The minimal polynomial of C_A is $A(y)$. Hence the algebra $J(A)$ generated by C_A over $\mathbb{F}_q$ is isomorphic to $\mathbb{F}_q[y]/(A(y))$. Since $f(x)$ is a permutation polynomial on $F_{n\times n}$, it is so on $J(A)$, and via the isomorphism is so on $\mathbb{F}_q[y]/(A(y))$. Now if $A(y) = \Pi p_i^{\alpha_i}(y)$, then $\mathbb{F}_q[y]/(A(y)) \simeq \oplus \sum \mathbb{F}_q[y]/(p_i^{\alpha_i}(y))$, and $f(x)$ permutes each of the $\mathbb{F}_q[y]/(p_i^{\alpha_i}(y))$. Taking $A(y)$ to have an irreducible factor of degree r and multiplicity one, we see that $f(x)$ permutes $\mathbb{F}_{q^r}$. Now if $A(y)$ has a factor of multiplicity greater than one, (and the degree of any such must be less than or equal to $[\frac{n}{2}]$), $f(x)$ must permute $\mathbb{F}_q[y]/(p_i^{\alpha_i}(y))$, $\alpha_i > 1$, deg $p_i(y) > r$. Such an $f(x)$ is called regular over $\mathbb{F}_q$, and it is known that regularity of f is equivalent to $f'(u) \neq 0$ for $u \in \mathbb{F}_{q^r}$. [See Lausch and Nöbauer [19] prop. 4.31 page 163].

Now assume $f(x)$ satisfies the given conditions. The similarity classes are determined by their invariant factors, which are polynomials in $\mathbb{F}_q[x]$.

A result from Gantmacher ([13], page 158, note 2,) ensures that the invariant factors of $f(A)$ are $\Delta_f g$, where g are the invariant factors of A, and Δ_f is the mapping defined in section 1. If $f(A) = f(B)$, where A,B are in different similarity classes, then if $\{g_i\}$ are the invariant factors of A, $\{h_j\}$ of B, the invariant factors of $f(A)$, $f(B)$ are $\{\Delta_f g_i\}$, $\{\Delta_f h_j\}$ respectively. Since the degrees of g_i, h_j are $\leq n$, and as by Theorem 1 Δ_f permutes the polynomials in $\mathbb{F}_q$ of each degree $\leq n$, $\{g_i\} = \{h_j\}$ and so A is similar to B, a contradiction. Thus f permutes the similarity classes, and so permutes $F_{n\times n}$ by Lemma 4.14. $\square$

CHAPTER 5

THE STRUCTURE OF THE GROUP OF PERMUTATIONS INDUCED BY CHEBYSHEV POLYNOMIAL VECTORS OVER THE RING OF INTEGERS MOD M

In this chapter we extend some of the results of chapter 4 to rings of the type $\mathbb{Z}/(m)$. Since the general case reduces to that of $m = p^e$, we shall study the case $m = p^e$, where p is prime, in detail. The structure of the group of permutations of $\mathbb{Z}/(m)$ induced by $\{g(n,k,1)\}$ was determined by Lausch, Müller and Nöbauer [18] for $n = 1$. The main result of this chapter is to extend this to an arbitrary number n of variables. The single variable case may be described as follows:

Let $G(p^e)$ denote the group of permutations of $(\mathbb{Z}/p^e)$ induced by the set $\{g(n,k,1)\}$. Then $G(p^e) \simeq A/K$, where

(i) if $p = 2$, $e \leq 2$, $A \simeq (\mathbb{Z}/(2^{e-1}.3))^*$,

(ii) if $p = 2$, $e \geq 3$, $A \simeq (\mathbb{Z}/(2^{e-2}.3))^*$,

(iii) if $p > 2$, $A \simeq (\mathbb{Z}/(p^{e-1} \cdot \frac{p^2-1}{2}))^*$,

and $K = \{1,-1\}$ if $e > 1$ or $p = 2$,

$K = \{1,-1,p,-p \bmod \frac{p^2-1}{2}\}$ if $e = 1$, $p > 2$.

The multivariable case may be stated more simply, although the proof is rather more complicated. We begin with a consideration of the Jacobian of the transformations involved, as this is related to their permutation properties mod p^e.

1. THE JACOBIAN OF $g^{(f)}$

The following result reduces the study of polynomials over $R = \mathbb{Z}/(p^e)$ to questions concerning finite fields. (See Lausch and Nöbauer, [19], prop 4.34, page 165). Let T be the ring of integers of an algebraic number field.

PROPOSITION 5.1. *Let* Q *be a primary ideal of* T *with associated prime ideal* P*,* $P \neq Q$*, and* T/Q *finite. Then a polynomial vector* $h = (h_1,\ldots,h_n)$, $h_i \in T[x_1,\ldots,x_n]$, *is a permutation polynomial vector over* T/Q *if and only if*

(i) h *is a permutation polynomial vector over* T/P*, and*

(ii) the Jacobian of h*,* ∂h*, is non-zero on* T/P.

A polynomial vector h over $\mathbb{F}_q (\simeq T/P)$ satisfying (i) and (ii) is called a regular polynomial vector over $\mathbb{F}_q$. We proceed to determine the regular polynomial vectors amongst the vectors $g^{(f)}$, and the $g(n,k,b)$.

If $\sigma_1,\ldots,\sigma_n \in \bar{\mathbb{F}}_q$, where $\bar{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$, define

$$S\colon (\sigma_1,\ldots,\sigma_n) \to (S_1(\sigma_1,\ldots,\sigma_n),\ldots,S_n(\sigma_1,\ldots,\sigma_n)) \tag{1}$$

where S_j is the j'th elementary symmetric function in $\sigma_1,\ldots,\sigma_n$. The map

$$g^{(f)}\colon S(\sigma_1,\ldots,\sigma_n) \to (S_1(f(\sigma_1),\ldots,f(\sigma_n)),\ldots,S_n(f(\sigma_1),\ldots,f(\sigma_n)))$$

is a well defined map of $\bar{\mathbb{F}}_q^n \to \bar{\mathbb{F}}_q^n$. If $\frac{\partial S}{\partial \sigma}$ denotes the Jacobian of S with respect to $\sigma = (\sigma_1,\ldots,\sigma_n)$ and if $Jg^{(f)}$ is the Jacobian of $g^{(f)}$, then

$$\frac{\partial S}{\partial \sigma} \cdot Jg^{(f)} = \frac{\partial}{\partial \sigma}\,(S(f(\sigma))) \tag{2}$$

where $f(\sigma) = (f(\sigma_1),\ldots,f(\sigma_n))$, since $g^{(f)}(S(\sigma)) = S(f(\sigma))$, and $\frac{\partial}{\partial \sigma}\,(g^{(f)}(S(\sigma)) = \frac{\partial S(\sigma)}{\partial \sigma} \cdot \frac{\partial g^{(f)}(S(\sigma))}{\partial (S(\sigma))} = \frac{\partial S}{\partial \sigma} \cdot Jg^{(f)}$.

The composition law for Jacobians yields

$$\frac{\partial}{\partial\sigma}\,(S(f(\sigma)) = \frac{\partial S}{\partial\sigma}\,(f(\sigma))\;.\;\frac{\partial f}{\partial\sigma}\;,$$

where $\frac{\partial S}{\partial\sigma}\,(f(\sigma))$ is the vector $\frac{\partial S}{\partial\sigma}$, with $f(\sigma_i)$ replacing σ_i. An explicit calculation shows that

$$\frac{\partial S}{\partial\sigma} = \prod_{\substack{i<j\\ i,j=1}}^{n} (\sigma_i - \sigma_j) \tag{3}$$

$$\frac{\partial S}{\partial\sigma}\,(f(\sigma)) = \prod_{\substack{i<j\\ i,j=1}}^{n} (f(\sigma_i) - f(\sigma_j))\;. \tag{4}$$

PROPOSITION 5.2. *The value of the Jacobian* $Jg^{(f)}$ *at* $(u_1,\ldots,u_n)$ *is given by*

$$Jg^{(f)}(u_1,\ldots,u_n) = \Big(\prod_{\substack{i<j\\ i,j=1}}^{n} \frac{f(\sigma_i)-f(\sigma_j)}{\sigma_i-\sigma_j}\Big)\Big(\prod_{i=1}^{n} f'(\sigma_i)\Big)\;,$$

where $\sigma_1,\ldots,\sigma_n$ *are the roots of*

$$r(u_1,\ldots,u_n,z) = z^n - u_1 z^{n-1} +\ldots+ (-1)^n u_n\;.$$

If $\sigma_i = \sigma_j$, $i \neq j$, *then the term* $(f(\sigma_i) - f(\sigma_j))/(\sigma_i - \sigma_j)$ *is to be interpreted as* $f'(\sigma_i)$.

PROOF. Only the last statement remains to be proved. There exists an algebraic number field K, with ring of integers A, and a prime ideal Q, with $A/Q \simeq \mathbb{F}_q$. Continuity in $\mathbb{C}$ shows that the formula of Proposition 5.2 should be interpreted as indicated when $\sigma_i = \sigma_j$. □

2. THE JACOBIAN OF g(n,k,b)

When $b = 0$, taking $f(z) = z^k$ in Proposition 5.2 yields the Jacobian of $g(n,k,0)$. We now assume that $b \neq 0$.

PROPOSITION 5.3. *Let* J_1 *be the Jacobian of the map*

$$S: (\sigma_1,\ldots,\sigma_{n+1}) \to (S_1(\sigma_1,\ldots,\sigma_{n+1}),\ldots,S_{n+1}(\sigma_1,\ldots,\sigma_{n+1})) ,$$

regarded as a form in $\sigma_1,\ldots,\sigma_{n+1}$ *and let* J_2 *be the Jacobian of the map*

$$S_b: (\sigma_1,\ldots,\sigma_n) \to (S_1(\sigma_1,\ldots,\sigma_{n+1}),\ldots,S_n(\sigma_1,\ldots,\sigma_{n+1}))$$

where $\sigma_1 \ldots \sigma_{n+1} = b$, $b \neq 0$. *Then* $J_2 = \frac{\sigma_{n+1}}{b} J_1 = \frac{\sigma_{n+1}}{b} \prod_{\substack{i<j\\ i,j=1}}^{n+1} (\sigma_i - \sigma_j)$.

PROOF. Consider the determinant

$$bJ_1 = \det \left(\sigma_j \frac{\partial S_i}{\partial \sigma_j}\right)_{(n+1)\times(n+1)}$$

Every entry of the last row of this determinant is b.

Thus $$J_1 = \det \left(\sigma_j \frac{\partial S_i}{\partial \sigma_j} - \sigma_{n+1} \frac{\partial S_i}{\partial \sigma_{n+1}}\right)_{n\times n} .$$

Since $$\sigma_1 \ldots \sigma_{n+1} = b, \quad \frac{\partial \sigma_{n+1}}{\partial \sigma_j} = - \frac{\sigma_{n+1}}{\sigma_j} .$$

Thus $$J_1 = \sigma_1 \ldots \sigma_n \det \left(\frac{\partial S_i}{\partial \sigma_j} + \frac{\partial \sigma_{n+1}}{\partial \sigma_j} \frac{\partial S_i}{\partial \sigma_{n+1}}\right) = \frac{b}{\sigma_{n+1}} J_2 . \quad \square$$

PROPOSITION 5.4. *The Jacobian* J *of* $g(n,k,b)$, $b \neq 0$, *is given by* $J = k^n \prod_{\substack{i<j\\ i,j=1}}^{n+1} \left(\frac{\sigma_i^k - \sigma_j^k}{\sigma_i - \sigma_j}\right)$, *where* J *is evaluated at* $(u_1,\ldots,u_n)$ *with*

$$r(u_1,\ldots,u_n,z) = (z - \sigma_1)\ldots(z - \sigma_{n+1}) \;.$$

If $\sigma_i = \sigma_j$, *then the corresponding term in the expression for* J *is* $k\sigma_i^{k-1}$.

PROOF. Since $\frac{\partial S}{\partial \sigma} J = \frac{\partial S}{\partial \sigma} (f(\sigma)) \frac{\partial f}{\partial \sigma}$,

we have $$\frac{\sigma_{n+1}}{b} \prod_{\substack{i<j \\ i,j=1}}^{n+1} (\sigma_i - \sigma_j) J = \frac{\sigma_{n+1}^k}{b^k} \prod_{\substack{i<j \\ i,j=1}}^{n+1} (\sigma_i^k - \sigma_j^j) k^n \prod_{i=1}^{n} \sigma_i^{k-1}$$

or $$J = k^n \prod_{\substack{i<j \\ i,j=1}}^{n+1} \frac{\sigma_i^k - \sigma_j^k}{\sigma_i - \sigma_j} . \qquad \square$$

3. REGULAR POLYNOMIAL VECTORS OVER FINITE FIELDS

THEOREM 5.1. $g^{(f)}$ *is a regular polynomial vector over* $\mathbb{F}_q$ *if and only if* $f(z)$ *is a regular polynomial over* $\mathbb{F}_{q^r}$, $1 \le r \le n$.

PROOF. It was shown in chapter 4 that the condition of the theorem is equivalent to $g^{(f)}$ being a permutation polynomial vector over $\mathbb{F}_q$, with the regularity condition omitted. If $f(z)$ is regular over $\mathbb{F}_{q^r}$, $1 \le r \le n$, then $f'(\sigma_i) \ne 0$, and $f(\sigma_i) - f(\sigma_j) \ne 0$, as f is a permutation polynomial over $\mathbb{F}_{q^r}$, $1 \le r \le n$. If $\sigma_i = \sigma_j$, the remark following Proposition 5.2 shows that in all cases $Jg^{(f)} \ne 0$. If $f(z)$ is not regular over $\mathbb{F}_{q^r}$, $1 \le r \le n$, then either $f'(\sigma) = 0$ for some $\sigma \in \mathbb{F}_{q^r}$, or $f(z)$ is not a permutation polynomial over $\mathbb{F}_{q^r}$. In the first case take $r(z) \in \mathbb{F}_q[z]$ to be monic of degree n with σ a root of $r(z)$ and take $u_1,\ldots,u_n$ to be the coefficients of

$g(z)$ with appropriate signs. Then from Proposition 5.2, $Jg^{(f)}(u_1,\ldots,u_n) = 0$. In the second case, $g^{(f)}$ is not a permutation polynomial vector over $\mathbb{F}_q$ by theorem 4.1. □

COROLLARY. $g^{(f)}$ *is regular over* $\mathbb{F}_q$ *if and only if* f *is a permutation polynomial over* $\mathbb{F}_{q^r}$, $1 \le r \le n$, *and* f' *has no irreducible factor of degree* $\le n$.

PROOF. If f' has an irreducible factor of degree $\le n$, then it has a zero in $\mathbb{F}_{q^r}$, $1 \le r \le n$, and so f is not regular over $\mathbb{F}_{q^r}$. Thus $g^{(f)}$ is not regular. □

4. REGULAR CHEBYSHEV POLYNOMIAL VECTORS

The following theorem may be found in Lausch and Nöbauer ([19], p. 209), and Lidl ([22]), for the cases $n = 1,2$ respectively.

THEOREM 5.2. $g(n,k,b)$ *is a regular polynomial vector over* $\mathbb{F}_q$, $q = p^e$, *if and only if* $b = 0$, $k = 1$ *or* $b \neq 0$ *and* $(k,p(q^s - 1)) = 1$, $s = 1,\ldots,n + 1$.

PROOF. For $b = 0$, the theorem follows from the Corollary to Theorem 5.1. If $b \neq 0$, and $g(n,k,b)$ is regular, then Proposition 5.4 shows that $(k,p) = 1$. Lidl and Wells [26] showed that $g(n,k,b)$, $b \neq 0$ is a permutation polynomial vector over $\mathbb{F}_q$ if and only if $(k,q^s - 1) = 1$ for $s = 1,\ldots,n + 1$. Thus we need only show that the conditions given ensure that the Jacobian of $g(n,k,b)$ is non-zero. Since $\sigma_i \neq 0$, $k\sigma_i^{k-1} \neq 0$. Further, the conditions given imply that x^k is a permutation polynomial over $\mathbb{F}_{q^s}$, $1 \le s \le n + 1$. Thus x^k permutes the set $\bigcup_{s=1}^{n+1} \mathbb{F}_{q^s}$, which shows that $J \neq 0$. □

5. THE STRUCTURE OF THE GROUP OF PERMUTATIONS OF $(\mathbb{Z}/(p^e))^n$ INDUCED BY THE SET $\{g(n,k,b),\ k \in \mathbb{Z}\}$.

Theorem 5.2 immediately shows that the group $G(n,b,p^e)$ of permutations of $R^n = (\mathbb{Z}/p^e)^n$ induced by polynomial vectors $g(n,k,b)$ with $b = 0$ is the one-element group. Henceforth, we assume $b = 1$. We proceed to find an integer ℓ such that the maps induced on R^n by $g(n,k,1)$ and $g(n,k + \ell,1)$ are identical. We denote $g(n,k,1)$ by $g(n,k)$ for convenience, and similarly $G(n,b,p^e)$ by $G(n)$ or $G(n,p^e)$. We have then a homomorphism $\psi\colon \mathbb{Z}_\ell^* \to G(n)$, where $\mathbb{Z}_\ell^*$ is the group of reduced residues mod ℓ, whose kernel is to be determined. Since each polynomial of degree $(n + 1)$ is a product of irreducible polynomials of degree at most $(n + 1)$, it is sufficient to show that $\Delta_{x^k} r = r$ (Δ_f as defined in chapter 4), where r is an irreducible polynomial of degree $n + 1$, which has constant term $(-1)^{n+1}$ if degree $r = n + 1$. Recalling that $R = \mathbb{Z}/(p^e)$, $e > 1$, there is a canonical homomorphism $\mu\colon R \to \mathbb{Z}/(p)$. We use various properties of Galois rings, which are given in chapter 1.

THEOREM 5.3. *Let $\beta \in \mathbb{Z}$ be defined by $p^{\beta-1} < n + 1 \le p^\beta$. If $\gamma = \mathrm{lcm}\,(p - 1,\dots,p^n - 1,(p^{n+1} - 1)/(p - 1))$, and $\ell = p^{e+\beta-2}\gamma$, then $g(n,k)$ and $g(n,k + \ell)$ induce the same map on R^n.*

PROOF. Let $f(x)$ be a monic irreducible polynomial over R. If $f(x)$ is a basic irreducible, (chapter 1) with deg $f(x) = r$, then $f(x)$ splits into linear factors over $GR(p^e,r)$. Each root is a unit, and so, if α is such a root, then $\alpha^{(p^r-1)p^{e-1}} = 1$, by lemma 1.4. If deg $f(x)$ is $(n + 1)$, then $f(x)$ has constant term $(-1)^{n+1}$. In $F_{p^{n+1}}$, μf has roots of order $\frac{p^{n+1}-1}{p-1}$. From the structure of $GR(p^e,n + 1)$ in lemma 1.4, α is a product of an element of order p^{e-1} and an element of G_1, and μ induces an isomorphism of G_1. Hence α satisfies $\alpha^{p^{e-1}(p^{n+1}-1)/(p-1)} = 1$.

If $f(x)$ is irreducible over R, but μf is reducible, we construct a ring extension of R in which $f(x)$ splits into linear factors $f(x) = \Pi(x - \alpha_i)$, with $\alpha_i^\ell = 1$. In $\mathbb{Z}/(p)$, μf is of the form $(h(x))^k$, where $h(x)$ is irreducible over $\mathbb{Z}/(p)$ (lemma 1.2). If deg $h(x) = s$, then $h(x)$ splits into linear factors over $\mathbb{F}_{p^s}$. Over $\mathbb{F}_{p^s}$, μf splits into factors of the form $\prod_{i=1}^{s} (x - \bar{\alpha}_i)^k$. By a form of Hensel's lemma (lemma 1.1), over $GR(p^e,s)$ $f(x)$ splits into factors, say $f(x) = f_1(x)\dots f_s(x)$, where $f_i(x) = (x - \alpha_i)^k + m_i(x)$ with $f_i(x) \in GR(p^e,s)[x]$, and where $m_i(x)$ has coefficients in the maximal ideal M of $GR(p^e,s)$. Using lemma 1.5, let K be an algebraic number field with ring of integers A, and P be a prime ideal in A, $P = pA$, with θ: $A/P^e \simeq GR(p^e,s)$. M is the image of P under θ. Let $F(x) \in A[x]$ be mapped onto $f_i(x)$ by θ, where $F(x)$ is of the form $(x - \alpha)^k + n(x)$, with θ: $n(x) \to m_i(x)$, θ: $\alpha \to \alpha_i$, and define S as the splitting field of $F(x)$ over K, T the ring of integers of S. Let $\eta_1,\dots,\eta_k$ be the roots of $F(x)$ in S. Let I be the ideal $(P^eT,P^{e-1}(\eta_1 - \alpha)T,\dots,P^{e-1}(\eta_k - \alpha)T)$, and define $W_e = T/I$. We show that $I \cap A = P^e$, and so there is a canonical embedding of R into W_e. For certainly $P^e \subseteq I \cap A$, while if $I \cap A \supset P^e$ then there is a proper ideal J in A with $P^e = (I \cap A)J$. Thus $I \cap A = P^t$, $t < e$, so $P^{e-1} \subseteq I \cap A$, and

$$P^{e-1}T \subseteq (I \cap A)T = I = P^eT + P^{e-1}(\eta_1 - \alpha)T + \ldots + P^{e-1}(\eta_k - \alpha)T \ .$$

$$\text{Hence } T \subseteq PT + (\eta_1 - \alpha)T + \ldots + (\eta_k - \alpha)T \qquad (*)$$

But $(\eta_i - \alpha)^k = -n(\eta_i) \in PT$, so $((\eta_i - \alpha)T)^k \subseteq PT$. If Q is a prime ideal of T dividing PT, then $Q|(\eta_i - \alpha)T$, so Q divides the RHS of $(*)$, and so $Q|T$, a contradiction.

Thus W_e is an extension ring of R. If $\overline{\eta}_i$ is the image of η_i in W_e, then $\overline{\eta}_i$ is a root of $f_i(x)$ and $f_i(x) = \prod_{j=1}^{k} (x - \overline{\eta}_j)$. We show that $\overline{\eta}_j^{\ell} = 1$. Firstly assume $e = 2$. Then

$$(\eta_j - \alpha)^k = -n(\eta_j) \in PT, \text{ and}$$

$$PT(\eta_j - \alpha) \subseteq I$$

Thus $(\overline{\eta}_j - \alpha_i)^{k+1} = 0$. Now $p^\beta \geq k + 1$, unless $k = n + 1 = p^\beta$ and so, except in this case, $(\overline{\eta}_j - \alpha_i)^{p^\beta} = 0$. Thus

$$\overline{\eta}_j^{p^\beta} = (\overline{\eta}_j - \alpha_i + \alpha_i)^{p^\beta} = (\overline{\eta}_j - \alpha_i)^{p^\beta} + \alpha_i^{p^\beta} = \alpha_i^{p^\beta} .$$

Since $\alpha_i \in GR(p^2,s)$, $\alpha_i^{p^\beta\gamma} = 1$, and so $\overline{\eta}_j^{p^\beta\gamma} = 1$. (If $k = n + 1$, the same argument as used previously may be employed to show that γ suffices). Thus in T, for $e = 2$,

$$\eta_i^{p^{\beta+e-2}\gamma} = 1 + \lambda + (\eta_1 - \alpha)\mu_1 + \ldots + (\eta_k - \alpha)\mu_k \ ,$$

$$\text{where } \lambda \in P^eT, \ \mu_j \in P^{e-1}T \ .$$

Arguing inductively, we raise this to the p'th power, to obtain

$$\eta_i^{p^{\beta+e-1}\gamma} - 1 \in p^{e+1}T + p^eT(\eta_1 - \alpha) + \ldots + p^eT(\eta_k - \alpha) \ .$$

In W_{e+1} we have then, $\eta_i^{p^{\beta+e-1}\gamma} = 1$.

Now suppose $k = n + 1 = p^\beta$. The roots $\bar{\eta}_i$ have order $p^{\beta+e-1}\gamma$, by the above argument. In fact $p^{\beta+e-2}\gamma$ suffices. Let S_r^n again denote the r'th elementary symmetric function in n variables. Then $A = \mathbb{Z}$, $P = p\mathbb{Z}$, and $f(x) = (x - \alpha)^{p^\beta} + pg(x)$. Assume firstly that $e = 2$. Then in W_e,

$$(\bar{\eta}_i - \alpha)^{p^\beta} = -pg(\eta_i)$$

$$\text{since } p(\bar{\eta}_i - \alpha) = 0,\ pg(\eta_i) = pg(\alpha) \ .$$

$$\text{Hence } \bar{\eta}_i^{p^\beta} = (\bar{\eta}_i - \alpha + \alpha)^{p^\beta} = (\bar{\eta}_i - \alpha)^{p^\beta} + \alpha^{p^\beta}$$

$$= \alpha^{p^\beta} - pg(\alpha).$$

For $e > 2$, lift to T, and raise to p'th powers successively to obtain

$$\bar{\eta}_i^{p^{\beta+e-2}} = \alpha^{p^{\beta+e-2}} + p^{e-1}h(\alpha)$$

$$\bar{\eta}_i^{\ell+k} = \bar{\eta}_i^{p^{\beta+e-2}\gamma+k} = (\alpha^{p^{\beta+e-2}} + p^{e-1}h(\alpha))^\gamma \bar{\eta}_i^k$$

$$= (\alpha^{p^{\beta+e-2}\gamma} + p^{e-1}h_1(\alpha))\bar{\eta}_i^k \ .$$

Since $\alpha \in \mathbb{Z}/(p^e)$, $\alpha^{p^{\beta+e-2}\gamma} = 1$, and so

$$\bar{\eta}_i^{\ell+k} = (1 + p^{e-1}h_1(\alpha))\bar{\eta}_i^k \ ,$$

$$S_r^{n+1}(\bar{\eta}_1^{\ell+k},\ldots,\bar{\eta}_{n+1}^{\ell+k}) = (1 + p^{e-1}h_1(\alpha))^r \ S_r^{n+1}(\bar{\eta}_1^k,\ldots,\bar{\eta}_{n+1}^k) \ .$$

Modulo p, f(x) has the form $(x - \alpha)^{p^\beta}$, and so the transformed polynomial is $(x - \alpha^k)^{p^\beta}$, whose coefficients are zero mod p, except for the final and initial terms. Thus

$$S_r^{n+1}(\bar{\eta}_1^k,\ldots,\bar{\eta}_{n+1}^k) \equiv 0 \text{ mod } p, \text{ and so}$$

$$S_r^{n+1}(\bar{\eta}_1^{\ell+k},\ldots,\bar{\eta}_{n+1}^{\ell+k}) \equiv S_r^{n+1}(\bar{\eta}_1^k,\ldots,\bar{\eta}_{n+1}^k) \text{ mod } p^e \ . \quad \square$$

6. DETERMINATION OF THE KERNEL OF ψ

As shown in §5, there is a homomorphism $\psi\colon \mathbb{Z}_\ell^* \to G(n)$, where $\mathbb{Z}_\ell^*$ is the multiplicative group of reduced residues mod ℓ, where ℓ is defined in theorem 5.3 and ψ is defined by

$$\psi\colon k \to \{\text{permutation induced on } R^n \text{ by } g(n,k,1), \text{ where } (k,\ell) = 1\}.$$

We asume $e \geq 2$, and since the case $n = 1$ was solved in [18], we assume $n \geq 2$. In the case $e = 1$, the kernel of ψ is non-trivial (see chapter 4) and if $e = 2$, $n = 1$, the kernel is $\{\underline{+}1\}$, as shown in [18]. For $n \geq 2$, $e \geq 2$, we shall show in this section that $\ker \psi = \{1\}$, and so ψ is an isomorphism.

LEMMA 5.1. *If* $k \in \operatorname{Ker} \psi$, *then* $k \equiv 1 \bmod \gamma$, *where*

$$\gamma = \operatorname{lcm}(p - 1,\ldots,p^n - 1,\frac{p^{n+1} - 1}{p - 1}) \ .$$

PROOF. Suppose $k \in \ker \psi$. Then

$$g(n,k)(u_1,\ldots,u_n) = (u_1,\ldots,u_n) \text{ for all } u_i \in Z/(p^e) \ .$$

From Taylor's formula (|19|, p. 268), if g_t denotes the t'th component of g(n,k), then

$$\begin{aligned} & g_t(u_1,\ldots,u_{j-1},u_j + p^{e-1},u_{j+1},\ldots,u_n) \\ & = g_t(u_1,\ldots,u_n) + p^{e-1}\frac{\partial g_t}{\partial u_j}(u_1,\ldots,u_n) . \end{aligned}$$

Thus $\frac{\partial g_t}{\partial u_j}(u_1,\ldots,u_n) = \delta_{tj} \bmod p$. Hence, if J is the Jacobian <u>matrix</u> of g(n,k), then

$$J(u_1,\ldots,u_n) = I_n \bmod p \text{ for all } u_i \in \mathbb{Z}/(p) .$$

Replacing J by I_n in the identity

$$J \cdot \left[\frac{\partial u_\ell}{\partial \sigma_i}\right] = \left[\frac{\partial g_\ell}{\partial \sigma_i}\right], \text{ we obtain}$$

$$\frac{\partial u_\ell}{\partial \sigma_i} = \frac{\partial g_\ell}{\partial \sigma_i} .$$

Taking $\ell = 1$, $\sigma_i - \sigma_{n+1} = k(\sigma_i^k - \sigma_{n+1}^k)$, so that $k\sigma_i^k - \sigma_i$ takes the same value for $i = 1,\ldots,n + 1$. If $\sigma_1,\ldots,\sigma_{n+1}$ are chosen not all equal, then $p \nmid k$. If $p = 2$, this shows $k \equiv 1 \bmod p$. If $p \neq 2$, choose $\sigma_1 = -\sigma_2 = \sigma(\neq 0,\ \sigma \in \mathbb{Z}/(p))$. Then $k\sigma^k = \sigma$. If $\sigma = 1$, then $k \equiv 1 \bmod p$. If $\sigma = \omega$, a primitive root mod p, then $k \equiv 1 \bmod (p - 1)$. Thus $(\sigma_i^k - \sigma_i)$ takes the same value, for $i = 1,\ldots,n + 1$. Now let ω be a primitive element of $\mathbb{F}_{p^r}$, $2 \leq r \leq n$, and let g(x) be its minimal polynomial over $\mathbb{F}_p$. If the constant term of g(x) is $(-1)^r\lambda$, define $f(x) = g(x)(x - \lambda^{-1})(x - 1)^{n-r}$. Take $\sigma_{n+1} = \lambda^{-1}$. Then $\omega^k - \omega = (\lambda^{-1})^k - (\lambda^{-1}) = 0$, since $\lambda^{-1} \in \mathbb{F}_p$. Thus $k \equiv 1 \bmod (p^r - 1)$, $1 \leq r \leq n$. If $r = n + 1$, take $\sigma = \omega^{p-1}$, to obtain

$$k \equiv 1 \bmod \frac{p^{n+1} - 1}{p - 1} .$$

Combining the congruences, we obtain

$$k \equiv 1 \bmod \gamma . \quad \square$$

Recall that $\beta \in \mathbb{Z}$ is defined by $p^{\beta-1} < n + 1 \leq p^{\beta}$.

<u>LEMMA 5.2</u>. If $\beta = 1$, then $k \in \ker \psi$ only if $k \equiv 1 \bmod p^{e-1}$.

<u>PROOF</u>. Let $f(x)$ have degree two, and constant term 1. We assume $n \geq 2$. Then $g(x) = (x - 1)^{n-1}f(x)$ has degree $(n + 1)$. If $k \in \operatorname{Ker} \psi$, then $k \equiv \pm 1 \bmod p^{e-1} (\frac{p^2 - 1}{2})$, by [18], Th. 3.6, p. 91, since p is odd $(n + 1 \leq p)$. Since $k \equiv 1 \bmod (p^2 - 1)$ by Lemma 5.1, the positive sign holds, and so $k \equiv 1 \bmod p^{e-1}$. $\square$

<u>LEMMA 5.3</u>. *If* $\beta \geq 2$ *and* $e = 2$ *then* $k \in \operatorname{Ker} \psi$ *only if* $k \equiv 1 \bmod p^{\beta}$.

<u>PROOF</u>. We construct a sequence $u_1,\ldots,u_n$ for which $g(n,k)(u_1,\ldots,u_n) \neq g(n,1)(u_1,\ldots,u_n)$ for $1 < k < p^{\beta} + 1$. It is sufficient to do this for the first components of the vectors $g(n,k)$, which we denote by g_k. We show that $u_1,\ldots,u_n$ may be chosen so that $g_k(u_1,\ldots,u_n) = g_1(u_1,\ldots,u_n) \Rightarrow k \equiv 1 \bmod p^{\beta}$.

Consider $f(x) = (x - 1)^{n+1} + pg(x)$, where $\deg g(x) \leq n$, and where $g(x)$ has zero constant term. We choose the coefficients of $g(x)$ to give us the required sequence. When reduced mod p, the corresponding sequence of g_k's is constant $(g_k = n + 1)$. If

$u_i = \binom{n+1}{i} + p\lambda_i$, then mod p^2 we obtain

$$g_k = (n + 1) + pk\{\binom{n+k-1}{n}\lambda_1 - \binom{n+k-2}{n}\lambda_2 +\ldots+ (-1)^{k+1}\lambda_k\},$$

for $k \leq n$. This follows from the recurrence for the g_k's given in Lidl [23], p. 183, namely

$$\begin{aligned} g_0 &= n + 1 \\ g_1 &= u_1 g_0 - nu_1 \\ &\vdots \\ g_n &= u_1 g_{n-1} - u_2 g_{n-2} +\ldots+ (-1)^{n-1} u_1 g_0 + (-1)^n u_n . \end{aligned}$$

Choose $\lambda_1 \not\equiv 0 \bmod p$, and $\lambda_2,\ldots,\lambda_{n-1}$ in turn such that $g_k(u_1,\ldots,u_n) \equiv n + 1 \bmod p^2$, $2 \leq k \leq n - 1$. Since $p^{\beta-1} < n + 1$, $n \geq p^{\beta-1}$. If $n > p^{\beta-1}$, choose λ_n in the same fashion. In this case, $g_k \not\equiv g_1$ if $k \leq n$. In particular, this holds for $k = 1 + p^{\beta-1}$. If $n = p^{\beta-1}$, then $g_n \equiv n + 1$, independent of λ_n. The coefficient of λ_n in g_{n+k} is $(-1)^{n+1}(n + k)\binom{n+k}{n}$. With $k = 1$, this gives

$$(-1)^{n+1}(n + 1)^2 \equiv (-1)^{n+1} \bmod p .$$

Thus λ_n may be chosen to give $g_{n+1}(u_1,\ldots,u_n) \equiv n + 1$, and so if $k = 1 + p^{\beta-1}$, then $k \notin \operatorname{Ker} \psi$.

Now consider $f(x)$ of the form

$$f(x) = [(x - 1)^{p^{\beta-1}} + ph(x)](x - 1)^{n+1-p^{\beta-1}}. \text{ (Note that } \beta \geq 2).$$

The sequence corresponding to $f(x)$ repeats with a period $p^{\beta-1}$ and by the argument above applied to the bracketed expression, $h(x)$ may be chosen so that

$$g_k(u_1,\ldots,u_n) \not\equiv g_1(u_1,\ldots,u_n), \text{ for } k \leq p^{\beta-1} .$$

Thus $k \equiv 1 \bmod p^{\beta-1}$ is a necessary condition. If $k \equiv 1 + tp^{\beta-1} \bmod p^{\beta}$, $1 \le t < p$, let $ts \equiv 1 \bmod p$. Then

$$k^s \equiv 1 + p^{\beta-1} \bmod p^{\beta} \ (\beta \ge 2) \ .$$

Since Ker ψ is a subgroup of $\mathbb{Z}_{\ell}^{*}$, if $k \in$ Ker ψ then $k^s \in$ Ker ψ, which is false. Thus the condition $k \equiv 1 \bmod p^{\beta}$ is necessary if $e = 2$. □

We note that lemma 5.3 immediately implies that the power of p occurring in the period of $\{g(n,k)\}$ is p^{β} when $e = 2$. To extend this to $e > 2$ we need to look at the case $e = 2$ more closely. For this purpose, define $f(x)$ as follows: If $p \nmid (n + 1)$, then

$$f(x) = (x - 1)^{n+1} + pg(x), \text{ where } (x - 1) \nmid g(x) \bmod p, \ \deg g \le n, \ g(0) = 0.$$

If $p \mid (n + 1)$, take

$$f(x) = (x - 1)^{n+1} + pg(x), \text{ where } (x - 1) \nmid g'(x) \bmod p, \ \deg g \le n, \ g(0) = 0.$$

<u>LEMMA 5.4</u>. *If* $(u_1,\ldots,u_n)$ *is the vector of coefficients of* $f(x)$ *defined above, then the period of the sequence* $\{g_k(u_1,\ldots,u_n)\}$ *is* p^{β} *over* $\mathbb{Z}/(p^2)$.

<u>PROOF</u>. For a fixed $(u_1,\ldots,u_n)$, $\{g_k\}$ is a linear recurring sequence. We apply results from Ward [45] to $\{g_k\}$. It should be noted that theorem 7.1 of Ward's earlier paper [44] on sequences of length three, and theorem 11.1 of [45], imply that the period of such a sequence mod p^N is $p^b\lambda$, where λ is the period mod p, and where $b \le N$. However, this is false, as shown by the sequences with which we are dealing. One must assume the sequence to be non-singular for these results to apply. We use Ward's fundamental

theorem [45], p. 606, which states that the period of a linear recurring sequence mod p^e is the least integer t such that

$$(x^t - 1)\ U(x) \equiv 0 \bmod (p^e, F(x)), \text{ where } F(x)$$

is the polynomial corresponding to the recurrence relation, and $U(x)$ depends on the initial terms. In the case of $\{g_k\}$, $F(x)$ is the generating polynomial $f(x)$ and $U(x)$ is $f'(x)$. The theorem also shows that the sequence is purely periodic. We show that $\{g_k\}$ has the required power of p as a period for suitable choice of $u_1,\ldots,u_n$. Take $f(x)$ as defined above. Then

$$(x - 1)f'(x) - (n + 1)f(x) = p[(x - 1)g'(x) - (n + 1)g(x)]\ .$$

Let $\ell \in Z$. Then

$$\begin{aligned}(x^{p^\ell} - 1)f'(x) - (n+1)\left(\frac{x^{p^\ell} - 1}{x - 1}\right)f(x) &= p\left(\frac{x^{p^\ell} - 1}{x - 1}\right)[(x - 1)g'(x) - (n+1)g(x)] \\ &= pk(x)\end{aligned}$$

Modulo p, $(x - 1)^{p^\ell - 1}$ divides $k(x)$ if $p \nmid (n + 1)$, and no higher power of $(x - 1)$ does so, and if $p \mid (n + 1)$, $k(x)$ is divisible by $(x - 1)^{p^\ell}$ and no higher power. Thus $pk(x) \equiv 0 \bmod (p^2, f(x))$ if and only if $p^\ell - 1 \geq n + 1$, or $p^\ell \geq n + 2$, if $p \nmid (n + 1)$, or $p^\ell \geq n + 1$ if $p \mid (n + 1)$. Thus the period of $\{g_k(u_1,\ldots,u_n)\}$ mod p^2 is

$$p^\beta, \text{ where } p^{\beta-1} < n + 1 \leq p^\beta\ . \quad \square$$

<u>LEMMA 5.5</u>. *The sequence* $\{g_k\}$ *of lemma 5.4 has period* $p^{e+\beta-2}$ over $\mathbb{Z}/(p^e)$.

PROOF. It is known that $p^{\beta+1}$ is a period for $\{g_k\}$ with $e = 3$. Assume p^{β} is likewise. Since $\beta \geq 2$, $pk(x) = p\left(\frac{x^{p^{\beta}}-1}{x^{p^{\beta-1}}-1}\right) k_1(x)$,

where $k(x)$ is as in the proof of lemma 5.5, and where $k_1(x)$ is divisible by $(x-1)^{p^{\beta-1}-1}$ mod p if $p \nmid (n+1)$ and by $(x-1)^{p^{\beta-1}}$ if $p \mid (n+1)$.

Case 1. Let $n + 1 < p^{\beta} - p^{\beta-1}$. Then $\frac{x^{p^{\beta}}-1}{x^{p^{\beta-1}}-1} = (x-1)^s f(x) + p\lambda(x)$,

where $s \geq 1$. If $x = 1$, $p = p\lambda(1)$, so $\lambda(1) \equiv 1$ mod p, and so $(x-1) \nmid \lambda(x)$ mod p. $p\left(\frac{x^{p^{\beta}}-1}{x^{p^{\beta-1}}-1}\right) k_1(x) = p^2\lambda(x)k_1(x) \bmod (p^3, f(x))$.

If this is zero, then $\lambda(x)k_1(x) \equiv 0 \bmod (p, f(x))$. But $\lambda(x)k_1(x)$ is divisible by $(x-1)^{p^{\beta-1}}$ or $(x-1)^{(p^{\beta-1}-1)}$ and no higher power, and $f(x) = (x-1)^{n+1}$ mod p, where $n + 1 > p^{\beta-1}$. Thus $\lambda(x)k_1(x) \not\equiv 0$ mod $(p, f(x))$, and so $\{g_k\}$ does not have period p^{β}.

Case 2. Let $n + 1 > p^{\beta} - p^{\beta-1}$. Then

$$\frac{x^{p^{\beta}}-1}{x^{p^{\beta-1}}-1} = (x-1)^{p^{\beta}-p^{\beta-1}} \bmod p ,$$

so $\frac{x^{p^{\beta}}-1}{x^{p^{\beta-1}}-1} = (x-1)^{p^{\beta}-p^{\beta-1}} + p\lambda(x)$, $\lambda(x) \in \mathbb{Z}[x]$, and $(x-1) \nmid \lambda(x)$ mod p.

If $s = (n+1) - (p^{\beta} - p^{\beta-1})$, then $s \geq 1$, and

$$(x-1)^s\, p\left(\frac{x^{p^{\beta}}-1}{x^{p^{\beta-1}}-1}\right) k_1(x) = p(-pg(x) + p(x-1)^s\lambda(x))k_1(x) \bmod (p^3, f(x)).$$

If $p\nmid(n + 1)$, then mod p, this is divisible precisely by $(x - 1)^{p^{\beta-1}-1}$. If $p|(n + 1)$, then $s > 1$, and since the greatest power of $(x - 1)$ dividing $g(x)$ is one, as $(x - 1)\nmid g'(x)$, the highest power of $(x - 1)$ occurring is $(x - 1)^{p^{\beta-1}+1}$. Thus in each case, the expression is not zero mod $(p^3,f(x))$.

Case 3. $n + 1 = p^{\beta} - p^{\beta-1}$. Choose $g(x)$ with $(x - 1)\nmid(g(x) - \lambda(x))$, where $\lambda(x)$ is defined as in Case 2, and $(x - 1)\nmid g'(x)$. Thus $(x - 1)|g(x)$, but $(x - 1)^2\nmid g(x)$ would suffice if $\deg g(x) \geq 2$, or $n + 1 \geq 3$, which is assumed. Thus the highest power of $(x - 1)$ occurring is $(x - 1)^{p^{\beta-1}}$, and $p^{\beta-1} < n + 1$.

To extend $e > 3$, multiply in turn by expressions of the form $\dfrac{x^{p^{\ell+1}}-1}{x^{p^{\ell}} - 1}$, where $\ell \geq \beta$. As in case 1, this is equal to $p\lambda(x)$ mod $f(x)$ where $(x - 1)\nmid\lambda(x)$ mod p. Thus for each higher power p^e of p, the power of p occurring in the order of $G(n)$ increases by one. If $n + 1 = p^{\beta+1} - p^{\beta}$, which can occur only if $p = 2$, $n + 1 = 2^{\beta}$, since $n + 1 \leq p^{\beta}$, then choose $g(x)$ as in case 3. The corresponding expression is

$$p^3(-g(x) + \lambda(x))(-g(x) + (x - 1)^{p^{\beta-1}}\lambda(x))k_1(x) ,$$

and by the choice of $g(x)$, $(p^{\beta-1} + 1)$ is the highest power of $(x - 1)$ occurring. Subsequent powers are dealt with as in case 1. □

<u>THEOREM 5.4</u>. *If* $e \geq 2$ *and* $n > 1$ *then the group* $G(n,p^e)$ *of permutations of* $(\mathbb{Z}/(p^e))^n$ *induced by polynomial vectors of the form* $g(n,k)$ *is isomorphic to the multiplicative group of reduced residues* mod ℓ, *where* $\ell = p^{e+\beta-2}\gamma$, $p^{\beta-1} < n + 1 \leq p^{\beta}$, *and*
$\gamma = \operatorname{lcm}(p - 1,\ldots,p^n - 1, \frac{p^{n+1} - 1}{p - 1})$.

<u>PROOF</u>. By theorem 5.3, the mapping $\psi\colon \mathbb{Z}_\ell^* \to G(n,p^e)$ is a surjective homomorphism. We show that Ker $\psi = \{1\}$. By lemma 5.1, if $k \in$ Ker ψ, then $k \equiv 1 \bmod \gamma$. Thus it suffices to show that $k \equiv 1 \bmod p^{e+\beta-2}$. If $\beta = 1$ this follows from lemma 5.2 and from lemma 5.3 if $\beta \geq 2$ and $e = 2$. If $\beta \geq 2$, $e > 2$, proceed by induction on e. If $k \equiv 1 \bmod p^{e+\beta-2}$ is a necessary condition for $k \in$ Ker ψ mod p^e, then mod p^{e+1}, the same condition is necessary for $k \in$ Ker ψ', where ψ' corresponds to ψ mod p^{e+1}. Thus $k \equiv 1 + tp^{e+\beta-2} \bmod p^{e+\beta-1}$. We show that $t \equiv 0 \bmod p$. If there exists $k \in$ Ker ψ' with $t \not\equiv 0 \bmod p$, and if $st \equiv 1 \bmod p$, then $k^s \equiv 1 + p^{e+\beta-2} \bmod p^{e+\beta-1}$. Thus $k' = 1 + p^{e+\beta-2} \in$ Ker ψ', and so

$$k'^t \in \text{Ker } \psi' \text{ for all } t \in Z .$$

Thus Ker $\psi' = \{1 + tp^{e+\beta-2}\} = \{k\colon k \equiv 1 \bmod p^{e+\beta-2}\}$. Thus $G(n,p^e) \simeq G(n,p^{e+1})$. By assumption $G(n,p^e) \simeq \mathbb{Z}_\ell^*$, and so there exists an isomorphism $\phi\colon \mathbb{Z}_\ell^* \to G(n,p^{e+1})$. Thus if $\alpha,\beta \in \mathbb{Z}$, $\alpha \equiv \beta \bmod \ell$, then $g(n,\alpha)$ and $g(n,\beta)$ induce the same map. By lemma 5.5, there is a sequence $\{g_k\}$ with period $p^{e+\beta-1}$ over $\mathbb{Z}/(p^{e+1})$. Thus the assumption $t \not\equiv 0 \bmod p$ has led to a contradiction, and so $t \equiv 0 \bmod p$. Thus $k \equiv 1 \bmod p^{e+\beta-1}$ is a necessary condition, completing the induction. $\square$

7. THE GENERAL CASE: $R = \mathbb{Z}/(m)$

We assume $n \geq 2$. For $n = 1$ see [18], section 6. Let $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ be the prime decomposition of m over $\mathbb{Z}$, and let $G(n,m)$ be the group of permutations of R induced by $\{g(n,k)\colon k \in \mathbb{Z}\}$. Let $\lambda_i = \operatorname{lcm}(p_i - 1, \ldots, p_i^n - 1, \frac{p_i^{n+1} - 1}{p_i - 1})$. If $\alpha_i = 1$, set $\mu_i = \lambda_i$. If $\alpha_i > 1$, set

$$\mu_i = p_i^{\alpha_i+\beta_i-2}\lambda_i, \text{ where } p_i^{\beta_i-1} < n + 1 \leq p_i^{\beta_i}.$$

Let $L = \operatorname{lcm}_{1\leq i\leq r} \{\mu_i\}$.

LEMMA 5.6. *If* $k \equiv \ell \bmod L$, *then the maps of* R^n *induced by* $g(n,k)$ *and* $g(n,\ell)$ *are equal.*

PROOF. If $k \equiv \ell \bmod L$ then $k \equiv \ell \bmod \mu_i$, $1 \leq i \leq r$. Thus by theorem 5.3 (in the case $\alpha_i \geq 2$) and by the corollary to theorem 4.4 (in the case $\alpha_i = 1$), $g(n,k)$ and $g(n,\ell)$ induce the same map on R_i^n, where $R_i = Z/(p_i^{\alpha_i})$. By the Chinese remainder theorem, $R \simeq \prod_{i=1}^{r} R_i$, and so $g(n,k)$ and $g(n,\ell)$ induce the same map on R^n. □

LEMMA 5.7. *The map* $\psi\colon \mathbb{Z}_L^* \to G(n,m)$ *defined by* $\psi(k) \to \{$*map of* R^n *induced by* $g(n,k)\}$ *is a homomorphism.*

PROOF. $g(n,k)$ is a permutation polynomial vector over $\mathbb{Z}/(m)$ if and only if $(k,L) = 1$. The rest follows from lemma 5.6. □

LEMMA 5.8. *The kernel of ψ, where ψ is defined in lemma 5.7, is a subgroup of the direct product of* t *copies of the cyclic group* C_{n+1} *of order* n + 1, *where* t *is the number of different prime factors of* m *with* $\alpha_i = 1$.

PROOF. If $k \in \operatorname{Ker} \psi$, then g(n,k) induces the identity map on $\mathbb{Z}/(p_i^{\alpha_i})$, $1 \le i \le r$. If $\alpha_i \ge 2$, then $k \equiv 1 \bmod \mu_i$. If $\alpha_i = 1$, then k is an element of the cyclic subgroup of order (n + 1) generated by p and μ_i, as shown in the corollary to theorem 4.4. The map $k \bmod L \to (k \bmod \mu_1, \ldots, k \bmod \mu_r)$ is the monomorphism of Ker ψ into $\prod_{i=1}^{r} \operatorname{Ker} \psi_i$, where $\psi_i = \psi|_{R_i}$ and $R_i = \mathbb{Z}/(p_i^{\alpha_i})$, and the result follows. □

In general the structure of G(n,m) depends on the interrelation of its prime factors. However, if all $\alpha_i \ge 2$ then we have

THEOREM 5.5. *If* $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ *and* $\alpha_i \ge 2$ *for* $1 \le i \le r$, *and* $n \ge 2$ *then* G(n,m), *the group of permutations of* $R^n = (\mathbb{Z}/(m))^n$ *induced by* {g(n,k)} *is isomorphic to the multiplicative group of reduced residues* mod L, *where*

$$L = \operatorname{lcm} \{\mu_i\}$$

$$\mu_i = p_i^{\alpha_i+\beta_i-2} \operatorname{lcm}(p_i - 1, \ldots, p_i^n - 1, \frac{p_i^{n+1} - 1}{p_i - 1}) ,$$

and

$$p_i^{\beta_i} < n + 1 \le p_i^{\beta} .$$

CHAPTER 6

THE SCHUR PROBLEM OVER ALGEBRAIC NUMBER FIELDS

One may ask which integral polynomials are permutation polynomials mod p for all primes p. Such a polynomial must be a linear polynomial ax + b, with $a \neq 0$. However, there are non-trivial polynomials f(x) which satisfy the condition that f is a permutation polynomial modulo infinitely many primes $p \in \mathbb{Z}$. The cyclic and Dickson polynomials defined in chapter 2 have this property. I. Schur conjectured that any polynomial satisfying this condition is a composition of polynomials of this special type, and proved a number of results in support of this conjecture. In [10] M. Fried confirmed Schur's conjecture in a more general form.

Let K be an algebraic number field with ring of integers A. If I is an ideal of A then a polynomial $f(x) \in A[x]$ induces a map $\bar{f}: A/I \to A/I$ defined by $\bar{f}(\alpha + I) = f(\alpha) + I$, for $\alpha \in A$.

DEFINITION 6.1. The polynomial $f(x) \in A[x]$ is called a permutation polynomial modulo I if $\bar{f}$ is a bijection of A/I.

Fried proved that any polynomial $f(x) \in A[x]$ which is a permutation polynomial mod P for infinitely many prime ideals P of A is a composition of cyclic and Chebyshev polynomials. The case $K = \mathbb{Q}$ is Schur's conjecture. Fried ([11]) has also considered the problem of determining all rational functions over $\mathbb{Q}$ which satisfy the Schur condition. This resulted in a classification of rational functions of prime degree which satisfy the Schur conjecture into five classes, one being the polynomial functions. The aim of this chapter is to describe, for a given algebraic number field K, precisely which compositions of cyclic and Chebyshev polynomials have the Schur property and, conversely, for which fields a given polynomial has the Schur property. The problem may be reduced to that of polynomials of the form $x^s \circ g_t(x)$, where $s,t \in \mathbb{Z}$. If $K = \mathbb{Q}$, then $x^s \circ g_t(x)$ has the Schur property if and only if $2 \nmid s$ and $(6,t) = 1$. Niederreiter and Lo ([32]) determined all polynomials of the form x^s or $g_t(x)$ which satisfy the Schur condition when K is a quadratic or cyclotomic field, and also solved the cyclic case for normal extensions of $\mathbb{Q}$ of odd degree. Since "most" polynomials of the form $x^s \circ g_t(x)$ satisfy the Schur condition for K, it is more convenient to describe those that do not. We call such a polynomial a *finite Schur polynomial for* K. All such polynomials can be constructed from certain polynomials which we call *primitive Schur polynomials*. Thus for $K = \mathbb{Q}$, the primitive Schur polynomials are x^2, $g_2(x)$, and $g_3(x)$. $f(x)$ is a finite Schur polynomial over $\mathbb{Q}$ if and only if $f(x)$ has one of these polynomials as a composition factor.

We begin by reducing the general case to that of an Abelian extension of $\mathbb{Q}$. To do this we use a theorem of Fried which depends ultimately on the Riemann hypothesis for curves over a finite field. The theorem may be used to deal with the case of polynomials of prime degree. We also give a proof of this case which uses only results from algebraic number theory. Similarly, the remainder of the chapter depends only on algebraic number theory and class field theory over $\mathbb{Q}$. We then consider the case of Abelian extensions of $\mathbb{Q}$, and finally some examples.

1. BASIC RESULTS.

Throughout the remainder of this chapter, K denotes an algebraic number field with ring of integers A. Capital letters P, Q, etc.

will denote prime ideals in A, small p, q, etc., primes of $\mathbb{Z}$. N(P) denotes the norm of P over $\mathbb{Q}$, sometimes written as $N_{K/\mathbb{Q}}(P)$. $\mathbb{Z}_n^*$ denotes the multiplicative group of reduced residues mod n.

PROPOSITION 6.1 *If* $f(x) = \alpha x^m + \beta$, *where* $\alpha, \beta \in K$, *then* f *is a permutation polynomial mod* P *if and only if* $(m, N(P)-1) = 1$, *and* α *is a unit mod* P.

PROOF. Theorem 2.3. □

PROPOSITION 6.2 *The Dickson polynomial* $g_m(x,\gamma)$, $\gamma \notin P$, *is a permutation polynomial mod* P *if and only if* $(m, (N(P))^2 - 1) = 1$.

PROOF. Theorem 2.1. □

We will need the following result from algebraic number theory. A proof may be found in Weil [46], p. 158, Prop. 15.

PROPOSITION 6.3. *Let* k, k', *be two extension fields of* $\mathbb{Q}$, *both contained in a separable extension* L *of finite degree over* $\mathbb{Q}$. *Let* X *be the set of primes* p *of* $\mathbb{Q}$ *such that* $|A/P| = p$, *for at least one prime* P *of* k *lying over* p, *where* A *is the ring of integers of* k. *If almost all the primes* $p \in X$ *split completely in* k', *then* $k' \subseteq k$.

PROPOSITION 6.4. *Let* $K = \mathbb{Q}(\zeta_p)$ *be the* p*'th cyclotomic field, where* p *is an odd prime. Then there exists a unique subfield* H_p *of* K *of degree* $(p-1)/2$ *over* $\mathbb{Q}$, *and the primes* q *of* $\mathbb{Q}$ *which split completely in* K *are those* $q \equiv \pm 1$ *mod* p.

PROOF. The existence and uniqueness of H_p follows from the fact that the Galois group of K is cyclic of order (p-1). If a prime q splits completely in K then it does so in H_p. If q has inertia degree 2 in K and is unramified then its inertia field is of degree (p-1)/2 and so is H_p. Thus q splits completely in H_p. Further, if q splits completely in H_p, then its inertia degree in K must be either 1 or 2. Hence the primes q which split completely in H_p are those which have inertia degree 1 or 2 in K. These are the primes q such that q has order 1 or 2 mod p. Thus $q^2 \equiv 1$ mod p, or $q \equiv \pm 1$ mod p. □

We may assume that $\alpha = \gamma = 1$, $\beta = 0$ in definitions 2.5 and 2.6.

DEFINITION 6.2. The polynomial $f(x) \in K[x]$ is a finite Schur polynomial for K if f(x) is a permutation polynomial over only finitely many residue class fields of K.

We are concerned with finding the finite Schur polynomials amongst those polynomials which are compositions of cyclic and Chebyshev polynomials.

PROPOSITION 6.5. *Let* $h = f_1 \circ g_1 \circ f_2 \circ g_2 \circ \ldots \circ f_k \circ g_k$ *be a composition of cyclic polynomials* f_i *and Chebyshev polynomials* g_j. *Let* $h' = (f_1 \circ \ldots \circ f_k) \circ (g_1 \circ \ldots \circ g_k)$. *Then* h *is a finite Schur polynomial if and only if* h' *is a finite Schur polynomial.*

PROOF. A composition of polynomials p_i is a permutation polynomial mod P if and only if each p_i is a permutation polynomial mod P. If P_f = {primes P: f is a p.p. mod P }, then $P_h = \cap P_f = P_{h'}$, where f ranges over the set $\{f_1,\ldots,f_k,g_1,\ldots,g_k\}$. Thus h[h'] is a finite Schur polynomial if and only if $P_h[P_{h'}]$ is finite. □

Thus we may restrict ourselves to polynomials of the form $x^s \circ g_t(x)$.

PROPOSITION 6.6. *The polynomial* $x^s \circ g_t(x)$ *is a finite Schur polynomial if and only if there are only finitely many primes* P *with* $(s, N(P) - 1) = (t, (N(P)^2 - 1) = 1$.

The following two lemmas are clear from the definitions.

LEMMA 6.1 . *If* $s|s'$, $t|t'$ *and* $x^s \circ g_t(x)$ *is a finite Schur polynomial for* K*, then so is* $x^{s'} \circ g_{t'}(x)$.

LEMMA 6.2. *If* $\mathbb{Q} \subseteq K \subseteq L$ *and* $x^s \circ g_t(x)$ *is a finite Schur polynomial for* K *then* $x^s \circ g_t(x)$ *is a finite Schur polynomial for* L.

DEFINITION 6.3. *A finite Schur polynomial for* K, $x^s \circ g_t(x)$, *is called a primitive Schur polynomial for* K *if there is no pair* (s',t') *with* $s'|s$, $t'|t$, $s't' < st$ *and* $x^{s'} \circ g_{t'}(x)$ *a finite Schur polynomial for* K.

LEMMA 6.3 *If* $x^s \circ g_t(x)$ *is a primitive Schur polynomial for* K *then* st *has distinct prime factors.*

PROOF. Let $s = \Pi p_i^{\alpha_i}$, $t = \Pi q_j^{\alpha_j}$. Then if $s' = \Pi p_i$, $t' = \Pi q_j$, $x^{s'} \circ g_{t'}(x)$ is a finite Schur polynomial if $x^s \circ g_t(x)$ is a finite Schur polynomial. If $k = \gcd(s,t) > 1$, then $x^{s/k} \circ g_{t/k}(x)$ is a finite Schur polynomial, so if $x^s \circ g_t(x)$ is primitive, then $k = 1$.

2. REDUCTION TO THE ABELIAN CASE

We need some results of Fried [11]. Let $K(x)$ be a rational function field over K, and $K(x,y)$ an extension of $K(x)$ by $f(y) - x$. Let $\widehat{K(x,y)}$ be a Galois closure of $K(x,y)$. Let $\hat{K}$ be the algebraic closure of K in $\widehat{K(x,y)}$. If $\tau \in \mathrm{Gal}(\hat{K}:K)$ let $\hat{K}^{(\tau)}$ be the fixed field of τ. Define $G(1) = \mathrm{Gal}(\widehat{K(x,y)}: \hat{K}(x,y))$, and $G(1,\tau) = \mathrm{Gal}(\widehat{K(x,y)}: \hat{K}^{(\tau)}(x,y))$. Then $\mathrm{Gal}(\widehat{K(x,y)}: K(x))$ acts as a permutation group on the roots $y = y_1,\dots,y_n$ of $(f(y) - x)$. Thus $G(1)$ and $G(1,\tau)$ act as permutation groups on $\{y_2,\dots,y_n\}$. Then (Fried [11], proposition 2.1) $f(x)$ induces a permutation of infinitely many residue class fields of K if and only if there exists $\tau \in \mathrm{Gal}(\hat{K}:K)$ such that each orbit of $G(1,\tau)$ on $\{y_2,\dots,y_n\}$ splits into strictly smaller orbits under the action of $G(1)$. (This result depends ultimately on the Riemann hypothesis for finite fields). If $f(x)$ is a composition of cyclic and Chebyshev polynomials, then f has rational integral coefficients, and so the construction above may be performed over $\mathbb{Q}$. Then $\hat{\mathbb{Q}} \subseteq \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n'th root of unity. Consider the diagram

$$\begin{tikzcd}
 & \hat{K} \arrow[rr] & & \hat{K}(x,y) \arrow[dd] \\
\hat{K}^{(\tau)} \arrow[ur] \arrow[rr] & & \hat{K}^{(\tau)}(x,y) \arrow[ur] & \\
K \arrow[u] \arrow[r] & K(x) \arrow[r] & K(x,y) \arrow[u] \arrow[r] & \widehat{K(x,y)}
\end{tikzcd}$$

If $\phi \in \mathrm{Gal}(\widehat{K(x,y)}: K(x))$, and $K' \subseteq K$, then the map rest: $\phi \to (\phi$ restricted to $\widehat{K'(x,y)})$ induces an isomorphism of

$\mathrm{Gal}(\widehat{K'(x,y)}: K'(x))$ to $\mathrm{Gal}(\widehat{K(x,y)}: K(x))$, and also of the subgroups occurring in the diagram. If we now take $K' = K \cap \hat{\mathbb{Q}}$, then $K \cap \hat{\mathbb{Q}} = \hat{\mathbb{Q}}$, and the restriction map induces an isomorphism of $\mathrm{Gal}(\hat{K}:K)$ to $\mathrm{Gal}(\hat{\mathbb{Q}}: K \cap \hat{\mathbb{Q}})$. Further, these isomorphisms preserve the permutation group action on $\{y_2,\ldots,y_n\}$. Thus we have shown

PROPOSITION 6.7. *The polynomial* $f(x)$ *is a finite Schur polynomial over* K *if and only if it is a finite Schur polynomial over* $K \cap \hat{\mathbb{Q}}$, *where* $\hat{\mathbb{Q}}$ *is a subfield of* $\mathbb{Q}(\zeta_n)$.

PROPOSITION 6.8. *The polynomial* $f(x)$ *is a finite Schur polynomial over* K *if and only if* $f(x)$ *is a finite Schur polynomial over the maximal Abelian subfield* A *of* K.

PROOF. If f is a finite Schur polynomial over A, then it is so over K. Conversely, if f is a finite Schur polynomial over K, then it is over $K \cap \hat{\mathbb{Q}}$. But $K \cap \hat{\mathbb{Q}}$ is Abelian over $\mathbb{Q}$, and so is contained in A. Thus f is a finite Schur polynomial over A. □

3. FINITE SCHUR POLYNOMIALS OF PRIME DEGREE

We now obtain criteria which effectively yield all finite Schur polynomials of prime degree over K.

THEOREM 6.1. *The cyclic polynomial* x^p, p *prime in* $\mathbb{Z}$, *is a finite Schur polynomial over* K *if and only if* K *contains* $\mathbb{Q}(\zeta_p)$, *where* ζ_p *is a primitive p'th root of unity.*

PROOF. Suppose $\mathbb{Q}(\zeta_p) \subseteq K$. In $L = \mathbb{Q}(\zeta_p)$, $N_{L/\mathbb{Q}}(Q) \equiv 1 \bmod p$, for all primes Q not lying over p. Since $N_{K/\mathbb{Q}}(Q)$ is a power of $N_{L/\mathbb{Q}}(Q \cap L)$, it follows that $N_{L/\mathbb{Q}}(Q) \equiv 1 \bmod p$, for all Q not lying over p.

Conversely, if x^p is a finite Schur polynomial, then we apply Proposition 6.3 with $k = K$, $k' = \mathbb{Q}(\zeta_p)$ and $L = Kk'$ (the compositum of k' and K). Then L is separable of finite degree, and X consists of those primes $q \in \mathbb{Z}$ for which there exists Q with $N_{K/\mathbb{Q}}(Q) = q$. For almost all such Q, $p|(q - 1)$, since x^p is a finite Schur polynomial. Hence $q \equiv 1 \bmod p$ for almost all $q \in X$. Thus q splits completely in $\mathbb{Q}(\zeta_p)$ for almost all $q \in X$ and so $\mathbb{Q}(\zeta_p) \subseteq K$ by Proposition 6.3. □

THEOREM 6.2. *The Chebyshev polynomial* $g_p(x)$, p *prime in* $\mathbb{Z}$, *is a finite Schur polynomial for* K *if and only if* $H_p \subseteq K$, *where* H_p *is defined in Proposition 6.4.*

PROOF. Suppose $H_p \subseteq K$. Since $H_p \subseteq L = \mathbb{Q}(\zeta_p)$, and is of index 2,

$$N_{L/\mathbb{Q}}(Q) = (N_{H_p/\mathbb{Q}}(Q \cap H_p))^2 .$$

Thus

$$(N_{H_p/\mathbb{Q}}(Q'))^2 \equiv 1 \bmod p, \text{ for all } q' \text{ not lying over } p.$$

Since $N_{L/\mathbb{Q}}(Q)$ is a power of $N_{H_p/\mathbb{Q}}(Q \cap H_p)$, it follows that $(N_{L/\mathbb{Q}}(Q))^2 \equiv 1 \bmod p$, and so $g_p(x)$ is a finite Schur polynomial.

Sufficiency is proved in the same way as in Theorem 6.1, taking $k' = H_p$. Then for almost all Q with $N_{K/\mathbb{Q}}(Q) = q$, $p|(q^2 - 1)$, since $g_p(x)$ is a finite Schur polynomial. Thus q splits completely in H_p for almost all $q \in X$ and so $H_p \subseteq K$ by proposition 6.3. □

We note that the results given above can also be deduced from Fried's theorem (§3). Thus in the cyclic case, $\hat{\mathbb{Q}} = \mathbb{Q}(\zeta_p)$, $G(1) = \{1\}$, and since $\mathrm{Gal}(\hat{\mathbb{Q}}: K \cap \hat{\mathbb{Q}})$ is cyclic, take $K^{(\tau)} = K \cap \mathbb{Q}(\zeta_p)$, where τ is a generator of $\mathrm{Gal}(\hat{\mathbb{Q}}: K \cap \hat{\mathbb{Q}})$. If x^p is a finite Schur polynomial over $K \cap \hat{\mathbb{Q}}$, there is an orbit of $G = \mathrm{Gal}(\widehat{K \cap \hat{\mathbb{Q}}(x,y)}: K \cap \hat{\mathbb{Q}}(x,y))$ which does not split further under the action of $G(1)$. Thus G fixes some $y_i = \zeta^{i-1}y$, and so fixes y_j, for $1 \le j \le p$. Thus

$$K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p) .$$

4. THE COMPOSITE CASE FOR ABELIAN EXTENSIONS OF $\mathbb{Q}$

Throughout this section, we assume that K is an Abelian extension of $\mathbb{Q}$. We recall the following well-known facts from class field theory over $\mathbb{Q}$ ([14]). By the Kronecker-Weber theorem, $K \subseteq \mathbb{Q}(\zeta_n)$, where n is the conductor of K. $\mathrm{Gal}(\mathbb{Q}(\zeta_n): \mathbb{Q}) \simeq \mathbb{Z}_n^*$, and if G_k is the subgroup of $\mathbb{Z}_n^*$ which fixes K, the primes of $\mathbb{Z}$ which split completely in K are the ones lying in those congruence classes mod n which are elements of G_K.

<u>LEMMA 6.4</u>. *If* $s|n$ *and* $t|n$ *and if, for each* $\ell \in G_K$, $\ell \equiv 1$ mod p *for some* p *dividing* s, *or* $\ell \equiv \underline{+}1$ mod q, *for some* q *dividing* t, *then* $x^s \circ g_t(x)$ *is a finite Schur polynomial over* K.

PROOF. The Galois group of K over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_n^*/G_K$. If P is a prime ideal of K lying over p, where p is unramified in K, then $N(P) = p^f$, where f is the order of the Frobenius automorphism of P. Thus the Artin map takes p^f to the identity element of $\mathbb{Z}_n^*/G_K$. Hence $N(P) \in G_K$, and so either $(s,N(P) - 1) > 1$ or $(t,n(P)^2 - 1) > 1$. Thus $x^s \circ g_t(x)$ is a finite Schur polynomial by Proposition 6.6. □

LEMMA 6.5. *If* $2 \nmid s$, $(6,t) = 1$ *and* $x^s \circ g_t(x)$ *is a primitive Schur polynomial over* K *then* $st|n$, *where* n *is the conductor of* K.

PROOF. Let $s = (\prod_{i\in I_s} p_i)(\prod_{j\in J_s} q_j)$, $t = (\prod_{i\in I_t} p_i)(\prod_{j\in J_t} q_j)$, where $p_i|n$, $q_j \nmid n$, and $J = J_s \cup J_t \neq \emptyset$. Since $q_j \neq 2$ if $j \in J_s$, $q_j \neq 2$ or 3 if $j \in J_t$, there exists $u \in \mathbb{Z}$ with u not congruent to 0 or 1 mod q_j, $j \in J_s$, u not congruent to 0 or ± 1 mod q_j, $j \in J_t$. If $I = I_s \cup I_t \neq \emptyset$, by lemma 6.4 there exists $\ell \in G_K$ such that $\ell \not\equiv 1 \bmod p_i$, for all $i \in I_s$, $\ell \not\equiv \pm 1 \bmod p_i$ for all $i \in I_t$, since otherwise $x^\alpha \circ g_\beta(x)$, with $\alpha = \prod_{i\in I_s} p_i$, $\beta = \prod_{i\in I_t} p_i$, would be a finite Schur polynomial, contradicting $J \neq \emptyset$ and $x^s \circ g_t(x)$ primitive. Any prime congruent to ℓ mod n splits completely in K. If $I = \emptyset$ choose $\ell = 1$. By Dirichlet's theorem there exist infinitely many primes $p \in \mathbb{Z}$ with $p \equiv \ell \bmod n$ and $p \equiv u \bmod (\prod_{j\in J} q_j)$. All such p have $N(P) = p$, where P lies over p. Thus there are infinitely many p with $(s,p - 1) = 1$ or $(t,p^2 - 1) = 1$, a contradiction. □

THEOREM 6.3. *Let* K *be an Abelian extension of* $\mathbb{Q}$ *with conductor* n, *and let* G_K *be the subgroup of* $\mathbb{Z}_n^*$ *which fixes* K. *If* $s \neq 2$, $t \neq 2$

or 3, *then* $x^s \circ g_t(x)$ *is a primitive Schur polynomial for* K *if and only if*

(i) $s = \prod_{j\in J_s} q_j$, $t = \prod_{j\in J_t} q_j$, *where* q_j *are distinct primes dividing* n, *and* $J_s \cap J_t = \phi$.

(ii) *If* $\lambda \in G_K$ *then* $\lambda \equiv 1 \bmod q_j$, $j \in J_s$ *or* $\lambda \equiv \pm 1 \bmod q_j$, $j \in J_t$, *for some* $j \in J = J_s \cup J_t$.

(iii) *If* $|J| \geq 2$, *then for each* $\alpha \in J$ *there exists* $\lambda \in G_K$ *with* $\lambda \not\equiv 1 \bmod q_\alpha$ *if* $\alpha \in J_s$ *or* $\lambda \equiv \pm 1 \bmod q_\alpha$ *if* $\alpha \in J_t$, *and* $\lambda \equiv 1 \bmod q_j$ *for* $j \in J_s$, $j \neq \alpha$, $\lambda \not\equiv \pm 1 \bmod q_j$, *for* $j \in J_t$, $j \neq \alpha$.

PROOF. Suppose (i) - (iii) hold. As in the proof of lemma 6.4, if P lies over $p \in \mathbb{Z}$, and p is unramified then $N(P) \in G_K$. Thus $(t,N(P) - 1) > 1$ or $(s,N(P)^2 - 1) > 1$ for almost all p. If $x^{s'} \circ g_{t'}(x)$ is exceptional, with s't' dividing st, then there are two cases to consider. Either $x^{s/q_\alpha} \circ g_t(x)$ or $x^s \circ g_{t/q_\alpha}(x)$ is exceptional, for some $\alpha \in J$. In the first case, by (iii) there exists $\lambda \in G_K$ with $\lambda \not\equiv 1 \bmod q_j$ for all q_j dividing (s/q_α) and $\lambda \not\equiv \pm 1 \bmod q_j$, for all q_j dividing t. There exist infinitely many rational primes congruent to λ mod n. These split completely, and so there are infinitely many prime ideals P with $(s/q_\alpha, N(P)-1)=1$ and $(t,N(P)^2 - 1) = 1$. Thus $x^{s/q_\alpha} \circ g_t(x)$ is not a finite Schur polynomial. The other case is similar. Thus $x^s \circ g_t(x)$ is primitive.

Suppose $x^s \circ g_t(x)$ is a primitive Schur polynomial, with $s \neq 2$, $t \neq 2$ or 3. By lemmas 6.3 and 6.5, $st|n$ and st has distinct prime factors, proving (i). Since $x^s \circ g_t(x)$ is a finite Schur polynomial, $(s,p-1) > 1$ or $(t,p^2-1) > 1$ for almost all primes p which split completely in K. Since the primes which split completely in K are uniformly distributed over G_K, (ii) holds. Suppose (iii) does not hold for $\alpha \in J$. Let (s',t') be defined by $s' = s/q_\alpha$ if $\alpha \in J_s$, $s' = s$ otherwise, $t' = t/q_\alpha$ if $\alpha \in J_t$, $t' = t$ otherwise. Then (i) and (ii) hold for $x^{s'} \circ g_{t'}(x)$, and so this is a finite Schur polynomial. Thus $x^s \circ g_t(x)$ is not primitive. □

5. EXAMPLES

We now apply the results of §2, 3 and 4 to various special cases.

PROPOSITION 6.9. *For any algebraic number field* K, x^2, $g_2(x)$ *and* $g_3(x)$ *are finite Schur polynomials.*

PROOF. We have $\mathbb{Q}(\zeta_2) = \mathbb{Q} \subseteq K$, and $H_3 = \mathbb{Q}$, since $[\mathbb{Q}(\zeta_3): \mathbb{Q}] = 2$. Theorems 6.1 and 6.2 then give the result. □

PROPOSITION 6.10. *If* $K = \mathbb{Q}$, *then* x^2, $g_2(x)$ *and* $g_3(x)$ *are the only primitive Schur polynomials for* K.

PROOF. If $p > 2$ then $\mathbb{Q}(\zeta_p) \nsubseteq \mathbb{Q}$, and $H_p \nsubseteq \mathbb{Q}$ if $p > 3$.

Since the conductor of $\mathbb{Q}$ is 1, theorem 6.3 shows that there are no composite primitive Schur polynomials. □

PROPOSITION 6.11. *The polynomial* $x^s \circ g_t(x)$ *is a primitive Schur polynomial only if all the prime factors of* s *other than* 2 *and of* t *other than* 2 *or* 3 *are ramified.*

PROOF. If $x^s \circ g_t(x)$ is of prime degree p, then $H_p \subseteq K$, and p is ramified in H_p if $p \neq 2$ or 3. If $t = 1$, then $\mathbb{Q}(\zeta_p) \subseteq K$, and p is ramified if $p \neq 2$. The composite case follows by reducing to the Abelian case and applying theorem 6.3 (i). □

We now examine the question of the existence of composite primitive Schur polynomials.

PROPOSITION 6.12. *If* K *is an Abelian extension of* $\mathbb{Q}$ *and* x^m *is a composite primitive Schur polynomial for* K *then* m *has at least three distinct prime factors.*

PROOF. Let $n = \prod_{i \in I} p_i^{\alpha_i}$, $m = p_1 p_2$, where n is the conductor of K. Then $\mathbb{Z}_n^* \simeq \oplus \prod_{i \in I} \mathbb{Z}/(p_i^{\alpha_i})$. If m is primitive exceptional then by theorem 6.3 (iii) G_K contains elements of the form $(\alpha, 1, \ldots)$ and $(1, \beta, \ldots)$ with $\alpha, \beta \neq 1$. Thus G_K contains $(\alpha, \beta, \ldots)$, contradicting theorem 6.3 (ii). □

COROLLARY. *If less than three primes ramify in* K*, where* K *is Abelian, then there are no composite primitive cyclic Schur polynomials for* K.

That composite primitive Schur polynomials exist is shown by the next two propositions.

PROPOSITION 6.13. *Let* $n = p_1p_2p_3$, *with* $p_i \neq 2$. *In* $\mathbb{Q}(\zeta_n)$ *there exists a unique subfield* K *such that* x^n *is a primitive Schur polynomial for* K. K *has index* 4 *in* $\mathbb{Q}(\zeta_n)$.

PROOF. Elementary considerations show that the only suitable subgroup G_K of $\mathbb{Z}_n^*$ is $\{(1,1,1), (1,\beta,\gamma), (\alpha,1,\gamma), (\alpha,\beta,1)\}$ where $\alpha,\beta,\gamma \equiv -1 \bmod p_1,p_2,p_3$, respectively. The corresponding subfield K of index 4 in $\mathbb{Q}(\zeta_n)$ has n as a primitive Schur polynomial. □

We note that the smallest degree of an example constructed above is 12.

PROPOSITION 6.14. *If* $m = \prod_{i=1}^{4} p_i$, *with* $p_i \equiv 1 \bmod 3$, *then there is a subfield of* $\mathbb{Q}(\zeta_n)$ *of index* 9 *in which* x^m *is a finite Schur polynomial.*

PROOF. In $\mathbb{Z}_{p_i}^*$ there is an element of order 3. If $\alpha,\beta,\gamma,\delta$, are such elements mod $p_1,\ldots,p_4$, then $G = \{(1,1,1,1), (1,\beta,\gamma,\delta), (1,\beta^2,\gamma^2,\delta^2), (\alpha,1,\gamma^2,\delta), (\alpha^2,1,\gamma,\beta^2), (\alpha,\beta,1,\delta^2), (\alpha^2,\beta^2,1,\delta), (\alpha,\beta^2,\gamma,1), (\alpha^2,\beta^2,\gamma^2,1)\}$ is a suitable subgroup. □

We now consider the cyclotomic and quadratic fields in the light of the general results of §2 and §3. These results have been obtained previously by Niederreiter and Lo [32].

PROPOSITION 6.15. *The polynomial* x^p(resp. $g_p(x)$), p *prime, is a finite Schur polynomial for* $\mathbb{Q}(\zeta_n)$ *if and only if* $p|2n$(resp. $p|6n$). *There are no composite primitive Schur polynomials.*

PROOF. We have $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_n)$ if and only if $p|n$ or $p = 2$. Similarly $H_p \subseteq \mathbb{Q}(\zeta_n)$ if and only if $p\ n$, $p = 2$ or $p = 3$. The conductor of $\mathbb{Q}(\zeta_n)$ is n. Thus $G_K = \{1\}$, and theorem 6.3 (iii) cannot hold for composite st. □

PROPOSITION 6.16. *The only cyclic Schur polynomial of prime degree for a quadratic field is* x^2 *unless* $K = \mathbb{Q}(\sqrt{-3})$, *when* x^3 *is a finite Schur polynomial. The only Chebyshev Schur polynomials of prime degree are* $g_2(x)$ *and* $g_3(x)$ *unless* $K = \mathbb{Q}(\sqrt{5})$ *in which case* $g_5(x)$ *is a finite Schur polynomial. There are no composite primitive Schur polynomials.*

PROOF. Since $[\mathbb{Q}(\zeta_3): \mathbb{Q}] = 2$, and $[\mathbb{Q}(\zeta_p): \mathbb{Q}] > 2$ if $p > 3$, the largest p with x^p a finite Schur polynomial is 3, and this can only occur if $K = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Similarly the largest possible H_p is H_5, and if this has degree two over $\mathbb{Q}$, then $K = H_5 = \mathbb{Q}(\sqrt{5})$. We now consider the composite case. Let $K = \mathbb{Q}(\sqrt{d})$, d squarefree, have conductor n, and suppose $x^s \circ g_t(x)$ is a finite Schur polynomial over K where st has at least two prime factors, $2\nmid s$, $(6,t) = 1$. By [5], page 504, $G_K = \{t \bmod n\colon (\frac{d}{t}) = 1\}$. If $d \equiv 1 \bmod 4$ then $n = |d|$, if $d \equiv 2$ or $3 \bmod 4$ then $n = 4|d|$. Let $d = (-1)^{\varepsilon_1} 2^{\varepsilon_2} d^*$, with $\varepsilon_i = 0$ or 1. Then

$$\left(\frac{d}{t}\right) = \left(\frac{-1}{t}\right)^{\varepsilon_1}\left(\frac{2}{t}\right)^{\varepsilon_2}\left(\frac{d^*}{t}\right) .$$

Let $s = \prod_{i\in I} p_i$, $t = \prod_{j\in J} p_j$, $I \cap J = \emptyset$, with $p_i | d^*$, $p_j \neq 3$, $j \in J$.

We construct $\lambda \in G_K$ with $\lambda \not\equiv 1 \bmod p_i$ for $i \in I$, $\lambda \not\equiv \pm 1 \bmod p_j$, $j \in J$, by the Chinese remainder theorem. If $q|d^*$, $q \nmid st$, let $\lambda \equiv 1 \bmod q$. We choose $\lambda \not\equiv 1 \bmod p_i$, $\lambda \not\equiv \pm 1 \bmod p_j$, for $i \in I$, $j \in J$. We further require $(\frac{\lambda}{p_i}) = 1$, $i \in I \cup J$. This is possible unless $3 \in \{p_i\}_{i \in I}$ or $5 \in \{p_j\}_{j \in J}$. If $p_1 = 3$, choose $\lambda \equiv 2 \bmod 3$, and $(\frac{\lambda}{p_2}) = -1$, $\lambda \not\equiv \pm 1 \bmod p_2$, if $2 \in J$, $\lambda \not\equiv 1 \bmod p_2$ if $2 \in I$. If $5 \in \{p_j\}_{j \in J}$, we take $p_2 = 5$. If $3 \not\equiv \{p_i\}_{i \in I}$, $5 \in \{p_j\}_{j \in J}$ we choose $\lambda \equiv 2 \bmod 5$ and $(\frac{\lambda}{p_2}) = -1$, for some $p_2 \neq 5$; with $\lambda \not\equiv 1 \bmod p_2$ or $\lambda \not\equiv \pm 1 \bmod p_2$, as appropriate. An extra condition is imposed on λ as follows.

<u>Case 1</u>. $\varepsilon_1 = \varepsilon_2 = 0$, $d^* \equiv 1 \bmod 4$.
No extra condition. $(\frac{d}{\lambda}) = 1$, λ is chosen mod $d^* = n$.

<u>Case 2</u>. $\varepsilon_1 = \varepsilon_2 = 0$, $d^* \equiv 3 \bmod 4$.
Choose $\lambda \equiv 1 \bmod 4$, then $(\frac{d}{\lambda}) = 1$, λ is chosen mod $4d^* = n$.

<u>Case 3</u>. $\varepsilon_1 = 1$, $\varepsilon_2 = 0$, $d^* \equiv 1 \bmod 4$.
Choose $\lambda \equiv 1 \bmod 4$, then $(\frac{d}{\lambda}) = (-\frac{1}{\lambda})(\frac{d^*}{\lambda}) = 1$, and λ is chosen mod $4d^* = n$.

<u>Case 4</u>. $\varepsilon_1 = 1$, $\varepsilon_2 = 0$, $d^* \equiv 3 \bmod 4$.
Choose $\lambda \equiv 3 \bmod 4$, $(\frac{d}{\lambda}) = (\frac{-1}{\lambda})(\frac{d^*}{\lambda}) = (-)(-)(\frac{\lambda}{d^*}) = (\frac{\lambda}{d^*}) = 1$, λ is chosen mod $4d^* = n$.

<u>Case 5</u>. $\varepsilon_2 = 1$. Choose $\lambda \equiv 1 \bmod 8$, then $\lambda \equiv 1 \bmod 4$.
Then $(\frac{d}{\lambda}) = (\frac{-1}{\lambda})^{\varepsilon_1}(\frac{2}{\lambda})(\frac{d^*}{\lambda}) = 1$. Here λ is chosen mod $8d^* = n$. □

Niederreiter and Lo [32] proved the next result for normal extensions of $\mathbb{Q}$ and cyclic or Chebyshev polynomials. By reducing to the Abelian case we may dispense with normality. The proof given by Niederreiter and Lo may be easily extended to yield

PROPOSITION 6.17. *If* $[K:\mathbb{Q}] = k$, *a necessary condition for* $x^s \circ g_t(x)$ *to be a finite Schur polynomial is that* $(p_i - 1)|k$ *for some* p_i *dividing* s, *or* $(q_j - 1)|2k$, *for some* q_j *dividing* t.

PROPOSITION 6.18. *Suppose* $[K:\mathbb{Q}]$ *is odd. Then* $x^s \circ g_t(x)$ *is a finite Schur polynomial only if* s *is even or* t *is divisible by a prime* p, *with* $p \equiv 3 \bmod 4$.

PROOF. $(p - 1)$ is even if $p \neq 2$. If $\frac{1}{2}(p - 1)$ is odd, then $p \equiv 3 \bmod 4$. □

PROPOSITION 6.19. *If* $[K:\mathbb{Q}] = 4$, *then* x^2 *is the only prime degree cyclic finite Schur polynomial unless* $\sqrt{-3} \in K$, *when* x^3 *is a finite Schur polynomial, or* $K = \mathbb{Q}(\zeta_5)$ *when* x^5 *is a finite Schur polynomial.* $g_2(x)$ *and* $g_3(x)$ *are the only Chebyshev Schur polynomials of prime degree unless* $\sqrt{5} \in K$, *when* $g_5(x)$ *is a finite Schur polynomial.*

CONCLUSION

Here we discuss certain unsolved problems and directions for further research.

In general it appears to be difficult to determine the permutation polynomials amongst polynomials of a given class. Such classes are usually defined by some analytic property, such as orthogonality, and not primarily by their coefficients. The criterion of Hermite, however, deals with the coefficients of a polynomial. Thus it would be of interest to relate the permutation properties of classes of polynomials to other properties, such as differential equations which may define them, etc. One approach may be to consider the polynomials p-adicly, and investigate the connection between polynomials which are p-adicly univalent and permutation polynomials of each type.

A further problem appears at the end of chapter 2. Classify all polynomials $f(x_1,\dots,x_n)$, $n > 1$, which are permutation polynomials over $\mathbb{F}_q$, for all $q = p^e$, $e \geq 1$. Does every elementary symmetric function which is a permutation polynomial over $\mathbb{F}_p$ have this property? All such polynomials have the same ζ-function, and so their behaviour over $\mathbb{C}$ may be relevant, through the Weil conjectures.

If, in the definitions beginning chapter 4, we take $r(z) = g_k(z)$, we obtain a class of multivariable polynomial vectors $h_k(z)$ whose permutation properties are similar to the $\{g(n,k,b)\}$. Do these polynomials have any nice analytic properties? What is the structure of the group of permutations they induce (they are closed under composition)? One could also pose these problems for rings $\mathbb{Z}/(p^e)$.

If one considers multivariable analogues of the Schur conjecture one may ask ([26]): which polynomial vectors over $\mathbb{Z}$ induce permutations of $\mathbb{F}_p^n$ for infinitely many primes p? The polynomial vectors $(z^{\alpha_1}, \ldots, z^{\alpha_n})$, the g(n,k,b)(z), and the $h_k(z)$ have this property. Are they compositionally independent and do they generate all such vectors? The problem concerning the elementary symmetric functions may be considered as an analogue of this problem.

BIBLIOGRAPHY

1. T. APOSTOL, Introduction to Analytic Number Theory, Springer, New York, 1976.

2. I. BLAKE and C. MULLIN, The Mathematical Theory of Coding, Academic Press, New York, 1975.

3. J. BRAWLEY, L. CARLITZ and J. LEVINE, Scalar polynomial functions on the n x n matrices over a finite field, Linear Algebra Appl. 10 (1975), pp. 199-217.

4. L. CARLITZ and J. HAYES, Permutations with coefficients in a subfield, Acta Arith. 21 (1972), pp. 131-135.

5. C.Y. CHAO, A note on block circulant matrices, Kyungpook Math. J. 14 (1) (1974), pp. 97-100.

6. P.J. DAVIS, Circulant Matrices, Wiley, New York, 1979.

7. L.E. DICKSON, History of the Theory of Numbers, Carnegie Institute, Washington, 1919.

8. L.E. DICKSON, Linear Groups, Dover Publications, New York, 1958.

9. R. EIER and R. LIDL, Tschebyscheffpolynome in einer und zwei Variablen. Abh. Math. Sem. Univ. Hamburg, 41 (1973), pp. 17-27.

10. M. FRIED, On a conjecture of Schur, Michigan Math. J. 17 (1980), pp. 41-55.

11. M. FRIED, Galois groups and complex multiplication, Trans. Amer. Math. Soc. 235 (1978), pp. 141-162.

12. B. FRIEDMAN, Eigenvalues of composite matrices, Proc. Cambridge Philos. Soc. 57 (1961), pp. 37-49.

13. G. GANTMACHER, The Theory of Matrices, Chelsea, New York, 1959.

14. A. GARBANATI, Class field theory summarized, Rocky Mountain J. Math. 11 No. 2 (1981), 195-225.

15. H. HASSE, Number Theory, Springer, Berlin, 1980.

16. K. HORAKOVA and S. SCHWARZ, Cyclic matrices and algebraic equations over finite fields, Mat.-Fyz. Cas. Sav. 12 (1) (1962), pp. 36-46.

17. H. HULE and W.B. MÜLLER, Grupos ciclicos de permutaciones inducidas por polinomios sobre campos de Galois, Anais da Academia Brasileira de Ciencias 44.

18. H. LAUSCH, W. MÜLLER, and W. NÖBAUER, Über die Struktur einer durch Dicksonpolynome dargestellten Permutationsgruppe des Restklassenringes modulo n, J. reine angew. Math. 261 (1973), pp. 88-99.

19. H. LAUSCH and W. NÖBAUER, Algebra of polynomials, North-Holland, Amsterdam, 1973.

20. R. LIDL, Tschebyscheffpolynome und die dadurch dargestellten Gruppen, Monatsh. Math. 77 (1973), pp. 132-147.

21. R. LIDL, Über die Struktur einer durch Tschebyscheffpolynome in 2 Variablen dargestellten Permutationsgruppe, Beiträge Algebra Geometrie 3 (1974), pp. 41-48.

22. R. LIDL, Reguläre Polynome über endlichen Körpern, Beiträge Algebra Geometrie 2 (1974), pp. 58-59.

23. R. LIDL, Tschebyscheffpolynome in mehreren Variablen, J. reine angew. Math. 273 (1975), pp. 178-198.

24. R. LIDL and H. NIEDERREITER, On orthogonal systems and permutation polynomials in several variables, Acta. Arith. 22 (1972), pp. 257-265.

25. R. LIDL and W. MÜLLER, Über Permutationsgruppen die durch Tschebyscheffpolynome erzeugt werden, Acta Arith. 30 (1976), pp. 19-25.

26. R. LIDL and C. WELLS, Chebyshev polynomials in several variables, J. reine angew, Math. 273 (1972), pp. 178-198.

27. B. McDONALD, Finite Rings with Identity, Dekker, New York, 1974.

28. W. NARKIEWICZ, Elementary and Analytic Theory of Algebraic Numbers, Polish Scientific Publishers, Warsaw, 1974.

29. H. NIEDERREITER, Permutation polynomials in several variables over finite fields, Proc. Japan Acad. 46 (1970), pp. 1001-1005.

30. H. NIEDERREITER, Orthogonal systems of polynomials in finite fields, Proc. Amer. Math. Soc. 28 (1971), pp. 415-422.

31. H. NIEDERREITER, Permutation polynomials in several variables, Acta Sci. Math. Szeged 33 (1972), pp. 53-58.

32. H. NIEDERREITER, and S. LO, Permutation polynomials over rings of algebraic integers, Abh. Math. Sem. Univ. Hamburg 49 (1979), 126-139.

33. W. NÖBAUER, Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen, J. reine angew. Math. 231 (1968), pp. 215-219.

34. O. ORE, Some studies on cyclic determinants, Duke Math. J. 18 (1951), pp. 343-354.

35. D. PASSMAN, Permutation Groups, Benjamin, New York, 1968.

36. G. RAUSSNITZ, Math. und Naturw. Berichte aus Ungarn. 1 (1882), pp. 275-278.

37. L. RÉDEI, Algebra, Pergamon, London, 1967.

38. S. SCHWARZ, On the number of irreducible factors of a polynomial over a finite field, Czechoslovak Math. J. 11 (1961), pp. 213-225 (Russian).

39. S. SCHWARZ, Note on algebraic equations over finite fields, Mat.-Fyz. Cas. Sav. 12 (3) (1962), pp. 224-229 (Russian).

40. J.A. SILVA, A theorem on cyclic matrices, Duke Math. J. 18 (1951), pp. 821-825.

41. R.L. SMITH, Moore-Penrose inverses of block circulant and block k-circulant matrices, Linear Algebra and Appl. 16 (1977), pp. 237-245.

42. G.E. TRAPP, Inverses of circulant matrices and block circulant matrices, Kyungpook Math. J. 13 (1) (1973), pp. 11-20.

43. T.P. VAUGHAN, Polynomials and linear transformations over finite fields, J. reine angew. Math. 267 (1974), pp. 179-206.

44. M. WARD, The characteristic number of a sequence of integers satisfying a linear recursion relation, Trans. Amer. Math. Soc. 33 (1931), pp. 153-165.

45. M. WARD, The arithmetical theory of linear recurring series, Trans. Amer. Math. Soc. 35 (1933), pp. 600-628.

46. A. WEIL, Basic Number Theory, Springer, New York, 1967.