J. Austral. Math. Soc. (*Series A*) **32** (1982), 88–103

THE STRUCTURE OF THE GROUP OF PERMUTATIONS INDUCED BY CHEBYSHEV POLYNOMIAL VECTORS OVER THE RING OF INTEGERS mod m

REX MATTHEWS

(Received 8 December 1980; revised 5 February 1981)

Communicated by R. Lidl

Abstract

In an earlier paper the author investigated the properties of a class of multivariable polynomial vectors which generalise the multivariable Chebyshev polynomial vectors. In this paper the behaviour of these polynomials over rings of the type $\mathbf{Z}/(m)$ is investigated, and conditions are determined for such an n-variable polynomial vector to induce a permutation of $(\mathbf{Z}/(m))^n$. More detailed results on the Chebyshev polynomial vectors follow. The composition properties of these vectors imply that the permutations induced by certain subsets of them form groups under composition of mappings, and the structure of these groups is investigated.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 12 C 05, 12 C 30.

1. Introduction

We begin by describing a class of multivariable polynomials whose properties are investigated in this paper. Let R denote the ring $\mathbf{Z}/(m)$, $m \in \mathbf{Z}$. Suppose that $f(z) \in R[z]$, and let

$$r(u_1, \ldots, u_n, z) = z^n - u_1 z^{n-1} + \ldots + (-1)^n u_n, \qquad u_i \in R.$$

In some extension ring of R, $r(z)$ splits into linear factors

$$r(u_1, \ldots, u_n, z) = (z - \sigma_1) \ldots (z - \sigma_n).$$

Define

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

Each $g_i^{(f)}$ is a symmetric function of $\sigma_1, \ldots, \sigma_n$, which is a polynomial in the elementary symmetric functions of $\sigma_1, \ldots, \sigma_n$, and so $g_i^{(f)}$ depends only on $u_1, \ldots, u_n$, and not on the particular factorisation of r. When $f(z) = z^k$, the vector $(g_1^{(f)}, \ldots, g_n^{(f)})$ is called a *Chebyshev polynomial vector*, as defined by Lidl and Wells [3]. When m is prime, or more generally when R is any finite field $\mathbf{F}_q$ of prime power order, the properties of the vectors $(g_1^{(f)}, \ldots, g_n^{(f)})$ have been investigated by the author [9]. In particular it was shown there that $\boldsymbol{g}_n^{(f)} = (g_1^{(f)}, \ldots, g_n^{(f)})$ induces a permutation of $\mathbf{F}_q^n$ (in this case we say that $\boldsymbol{g}_n^{(f)}$ is a *permutation polynomial vector* over $\mathbf{F}_q$) if an only if $f(z)$ is a permutation polynomial over $\mathbf{F}_{q^r}$, $1 \leqslant r \leqslant n$. In the first part of this paper we extend these results to the rings $\mathbf{Z}/(m)$. 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.

We also consider a similar construction, where the constant term of $r(z)$ is fixed. Thus over R let

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

Let

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

This defines a polynomial vector

$$\boldsymbol{g}(n, k, b) = \left(g_1^{(k)}(u_1, \ldots, u_n, b), \ldots, g_n^{(k)}(u_1, \ldots, u_n, b)\right).$$

When $b = 0$, we essentially obtain $\boldsymbol{g}_{n-1}^{(f)}$, with $f(z) = z^k$. In case R is a finite field $\mathbf{F}_q$, it was shown by Lidl and Wells [3] that the set $\{\boldsymbol{g}(n, k, b); k \in \mathbf{Z}\}$ is closed under polynomial composition if and only if $b = 0, +1$ or -1. The structure of the group of permutations of $\mathbf{F}_q^n$ induced by $\{\boldsymbol{g}(n, k, b)\}$ was determined by Nöbauer ([11]) for $n = 1$, Lidl ([4] and [5]) for $n = 2$, and by the author [9] for arbitrary n. For rings of the type $\mathbf{Z}/(p^e)$, (and more generally for $\mathbf{Z}/(m)$, $m \in \mathbf{Z}$) the corresponding group structure has been determined by Lausch, Müller and Nöbauer [1] for $n = 1$. The main result of this paper is to extend this to an arbitrary number n of variables.

https://doi.org/10.1017/S1446788700024435 Published online by Cambridge University Press

2. The Jacobian of $g^{(f)}$

The following result reduces the study of polynomials over $R = \mathbf{Z}/(p^e)$ to questions concerning finite fields. (See Lausch and Nöbauer, [2], Proposition 4.34, p. 165.) Let T be the ring of integers of an algebraic number field.

PROPOSITION 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 $\boldsymbol{h} = (h_1, \ldots, h_n)$, $h_i \in T[x_1, \ldots, x_n]$, is a permutation polynomial vector over T/Q if and only if*

(i) *$\boldsymbol{h}$ is a permutation polynomial vector over T/P, and*

(ii) *the Jacobian of $\boldsymbol{h}$, $\partial\boldsymbol{h}$, is non-zero on T/P.*

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

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

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

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

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

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

$$\frac{\partial \boldsymbol{S}}{\partial \boldsymbol{\sigma}} \cdot J\boldsymbol{g}^{(f)} = \frac{\partial}{\partial \boldsymbol{\sigma}}(\boldsymbol{S}(\boldsymbol{f}(\boldsymbol{\sigma}))) \tag{2}$$

where $\boldsymbol{f}(\boldsymbol{\sigma}) = (f(\sigma_1), \ldots, f(\sigma_n))$, since $\boldsymbol{g}^{(f)}(\boldsymbol{S}(\boldsymbol{\sigma})) = \boldsymbol{S}(\boldsymbol{f}(\boldsymbol{\sigma}))$, and

$$\frac{\partial}{\partial \boldsymbol{\sigma}}(\boldsymbol{g}^{(f)}(\boldsymbol{S}(\boldsymbol{\sigma}))) = \frac{\partial \boldsymbol{S}(\boldsymbol{\sigma})}{\partial \boldsymbol{\sigma}} \cdot \frac{\partial \boldsymbol{g}^{(f)}(\boldsymbol{S}(\boldsymbol{\sigma}))}{\partial(\boldsymbol{S}(\boldsymbol{\sigma}))} = \frac{\partial \boldsymbol{S}}{\partial \boldsymbol{\sigma}} \cdot J\boldsymbol{g}^{(f)}.$$

The composition law for Jacobians yields

$$\frac{\partial}{\partial \boldsymbol{\sigma}}(\boldsymbol{S}(\boldsymbol{f}(\boldsymbol{\sigma}))) = \frac{\partial \boldsymbol{S}}{\partial \boldsymbol{\sigma}}(\boldsymbol{f}(\boldsymbol{\sigma})) \cdot \frac{\partial \boldsymbol{f}}{\partial \boldsymbol{\sigma}},$$

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

$$\begin{aligned} \frac{\partial \boldsymbol{S}}{\partial \boldsymbol{\sigma}} &= \prod_{\substack{i<j \\ i,j=1}}^{n} (\sigma_i - \sigma_j), \\ \frac{\partial \boldsymbol{S}}{\partial \boldsymbol{\sigma}}(\boldsymbol{f}(\boldsymbol{\sigma})) &= \prod_{\substack{i<j \\ i,j=1}}^{n} (f(\sigma_i) - f(\sigma_j)). \end{aligned} \tag{3}$$

https://doi.org/10.1017/S1446788700024435 Published online by Cambridge University Press

PROPOSITION 2. *The value of the Jacobian* $Jg^{(f)}$ *at* $(u_1, \ldots, u_n)$ *is given by*

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

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 $A/Q \simeq \mathbf{F}_q$. Continuity in $\mathbf{C}$ shows that the formula of Proposition 2 should be interpreted as indicated when $\sigma_i = \sigma_j$.

3. The Jacobian of $g(n, k, b)$

When $b = 0$, taking $f(z) = z^k$ in Proposition 2 yields the Jacobian of $g(n, k, 0)$. We now assume that $b \neq 0$.

PROPOSITION 3. *Let* J_1 *be the Jacobian of the map*

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

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

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

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

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

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

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

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

$$J_1 = \sigma_1 \ldots \sigma_n \det(\partial S_i/\partial \sigma_j + \partial \sigma_{n+1}/\partial \sigma_j \cdot \partial S_i/\partial \sigma_{n+1}) = (b/\sigma_{n+1}) J_2.$$

https://doi.org/10.1017/S1446788700024435 Published online by Cambridge University Press

PROPOSITION 4. *The Jacobian J of $\mathbf{g}(n, k, b)$, $b \neq 0$, 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 $(\partial \boldsymbol{S}/\partial \boldsymbol{\sigma})J = (\partial \boldsymbol{S}/\partial \boldsymbol{\sigma})(\boldsymbol{f}(\boldsymbol{\sigma}))\partial \boldsymbol{f}/\partial \boldsymbol{\sigma}$, we have

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

or

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

4. Regular polynomial vectors over finite fields

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

PROOF. It was shown in [9] that the condition of the theorem was equivalent to $\mathbf{g}^{(f)}$ being a permutation polynomial vector over $\mathbf{F}_q$, with the regularity condition omitted. If $f(z)$ is regular over $\mathbf{F}_{q^r}$, $1 \leqslant r \leqslant n$, then $f'(\sigma_i) \neq 0$, and $f(\sigma_i) - f(\sigma_j) \neq 0$, as f is a permutation polynomial over $\mathbf{F}_{q^r}$, $1 \leqslant r \leqslant n$. If $\sigma_i = \sigma_j$, the remark following Proposition 2 shows that in all cases $J\mathbf{g}^{(f)} \neq 0$. If $f(z)$ is not regular over $\mathbf{F}_{q^r}$, $1 \leqslant r \leqslant n$, then either $f'(\sigma) = 0$ for some $\sigma \in \mathbf{F}_{q^r}$, or $f(z)$ is not a permutation polynomial over $\mathbf{F}_{q^r}$. In the first case take $r(z) \in \mathbf{F}_q[z]$ 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 2, $J\mathbf{g}^{(f)}(u_1, \ldots, u_n) = 0$. In the second case, $\mathbf{g}^{(f)}$ is not a permutation polynomial vector over $\mathbf{F}_q$ by Theorem 1 of [9].

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

https://doi.org/10.1017/S1446788700024435 Published online by Cambridge University Press

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

5. Regular Chebyshev polynomial vectors

The following theorem may be found in Lausch and Nöbauer ([2], p. 209), and Lidl ([6]), for the cases $n = 1, 2$, respectively.

THEOREM 2. *$\boldsymbol{g}(n, k, b)$ is a regular polynomial vector over $\mathbf{F}_q$, $q = p^e$, 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 1. If $b \neq 0$, and $\boldsymbol{g}(n, k, b)$ is regular, then Proposition 4 shows that $(k, p) = 1$. Lidl and Wells [3] showed that $\boldsymbol{g}(n, k, b)$, $b \neq 0$ is a permutation polynomial vector over $\mathbf{F}_q$ 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 $\boldsymbol{g}(n, k, b)$ 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 $\mathbf{F}_{q^s}$, $1 \leqslant s \leqslant n + 1$. Thus x^k permutes the set $\bigcup_{s=1}^{n+1} \mathbf{F}_{q^s}$, which shows that $J \neq 0$.

6. The structure of the group of permutations of $(\mathbf{Z}/(p^e))^n$ induced by the set $\{\boldsymbol{g}(n, k, b), k \in \mathbf{Z}\}$

Theorem 2 immediately shows that the group $G(n, b, p^e)$ of permutations of $R^n = (\mathbf{Z}/p^e)^n$ induced by polynomial vectors $\boldsymbol{g}(n, k, b)$ 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 $\boldsymbol{g}(n, k, 1)$ and $\boldsymbol{g}(n, k + l, 1)$ are identical. We denote $\boldsymbol{g}(n, k, 1)$ by $\boldsymbol{g}(n, k)$ for convenience, and similarly $G(n, b, p^e)$ by $G(n)$ or $G(n, p^e)$. We have then a homomorphism ψ: $\mathbf{Z}_l^* \to G(n)$, where $\mathbf{Z}_l^*$ 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 section 1), where r is an irreducible polynomial of degree $\leqslant n + 1$, which has constant term $(-1)^{n+1}$ if degree $r = n + 1$. Recalling that $R = \mathbf{Z}/(p^e)$, $e > 1$, there is a canonical homomorphism μ: $R \to \mathbf{Z}/(p)$. If $\mu(r)$ is irreducible over $\mathbf{Z}/(p)$, then r is called a basic irreducible. All rings of the form $R[x]/(f(x))$, where $f(x)$ is a basic irreducible, of degree t, are isomorphic, and such a ring is known as a Galois ring $GR(p^e, t)$, where $t = \deg f$. In $GR(p^e, t)$, $f(x)$ splits uniquely into

https://doi.org/10.1017/S1446788700024435 Published online by Cambridge University Press

linear factors. Results on Galois rings may be found in McDonald [8], Chapter XVI. The group of units of $GR(p^e, t)$ is known and can be described as follows, ([8], p. 322).

PROPOSITION 5. *Let $T = GR(p^e, t)$, 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 $p^{(e-1)t}$, such that*

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

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

THEOREM 3. *Let $\beta \in \mathbf{Z}$ be defined by $p^{\beta-1} < n + 1 \leqslant p^\beta$. If*

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

and $l = p^{e+\beta-2}\gamma$, then $\mathbf{g}(n, k)$ and $\mathbf{g}(n, k + l)$ induce the same map on R^n.

For the proof we shall need the following lemma.

LEMMA 1. *There is a finite algebraic extension K of $\mathbf{Q}$, with ring of integers O, and a prime ideal P with $P = pO$, such that*

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

PROOF. Let $f(x)$ be an irreducible monic polynomial of degree t over $\mathbf{Z}$ such that $\mu f(x)$ is irreducible over $\mathbf{Z}/(p)$. If α is a root of μf in $\mathbf{F}_{q^t}$, then $\mu f'(\alpha) \neq 0$. Thus $\operatorname{disc}(\mu f) \neq 0$ in $\mathbf{Z}_p$, and so $p \nmid \operatorname{disc} f$ over $\mathbf{Z}$. By the Kummer-Dedekind theorem on ideal factorisation (see [10], p. 161) p remains inert in $K = \mathbf{Q}[x]/(f(x))$. If O is the ring of integers of K, let $S = O/P^e$, where $P = pO$. Then $\operatorname{char} S = p^e$, 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 $\mathbf{Z}/(p^e)$. S is clearly a commutative local ring, $[O/P: \mathbf{Z}/(p)] = t$, and so S contains a subring $T \simeq GR(p^e, t)$, by McDonald [8], Theorem XVII.1, p. 337. Since $|S| = p^{et} = |T|$, $S = T$, which completes the proof of Lemma 1.

PROOF OF THEOREM 3. Let $f(x)$ be a monic irreducible polynomial over R. If $f(x)$ is a basic irreducible, 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 Proposition 5. If $\deg f(x)$ is $(n + 1)$, then $f(x)$ has constant term $(-1)^{n+1}$. In $\mathbf{F}_{p^{n+1}}$, μf has roots of order $(p^{n+1} - 1)/(p - 1)$. From the structure of $GR(p^e, n + 1)$ in Proposition 5, 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, $f(x) = \prod(x - \alpha_i)$, with $\alpha_i^l = 1$. In $\mathbf{Z}/(p)$, μf is of the form $(h(x))^t$, where $h(x)$ is irreducible over $\mathbf{Z}/(p)$ ([8], Theorem XIII.7, p. 260). If deg $h(x) = s$, then $h(x)$ splits into linear factors over $\mathbf{F}_{p^s}$. Over $\mathbf{F}_{p^s}$, μf splits into factors of the form $\prod_{i=1}^{s}(x - \bar{\alpha}_i)^k$. By a form of Hensel's lemma ([8], Theorem XIII.4, p. 256), over $GR(p^e, s)$ $f(x)$ splits into factors, say $f(x) = f_1(x) \ldots f_s(x)$, where $f_i(x) = (x - \alpha_i)^t + m_i(x)$ 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, let K be an algebraic number field with ring of integers O, and P be a prime ideal in O, $P = pO$, with θ: $O/P^e \simeq GR(p^e, s)$. M is the image of P under θ. Let $F(x) \in O[x]$ 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 $\eta_1, \ldots, \eta_k$ be the roots of $F(x)$ in S. Let I be the ideal $(P^eT, P^{e-1}(\eta_1 - \alpha)T, \ldots, P^{e-1}(\eta_k - \alpha)T)$, and define $W_e = T/I$. We show that $I \cap O = P^e$, and so there is a canonical embedding of R into W_e. For certainly $P^e \subseteq I \cap O$, while if $I \cap O \supset P^e$ then there is a proper ideal J in O with $P^e = (I \cap O)J$. Thus $I \cap O = P^t$, $t < e$, so $P^{e-1} \subseteq I \cap O$, and

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

Hence

$$(*) \qquad T \subseteq PT + (\eta_1 - \alpha)T + \ldots + (\eta_k - \alpha)T.$$

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 $\bar{\eta}_i$ is the image of η_i in W_e, then $\bar{\eta}_i$ is a root of $f_i(x)$ and $f_i(x) = \prod_{j=1}^{k}(x - \bar{\eta}_j)$. We show that $\bar{\eta}_j^l = 1$. Firstly assume $e = 2$. Then

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

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

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

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

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

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

https://doi.org/10.1017/S1446788700024435 Published online by Cambridge University Press

Arguing inductively, we raise this to the pth 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 rth elementary symmetric function in n variables. Then $O = \mathbf{Z}$, $P = p\mathbf{Z}$, and $f(x) = (x - \alpha)^{p^\beta} + pg(x)$. Assume firstly that $e = 2$. Then in W_e,

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

since $p(\bar{\eta}_i - \alpha) = 0, pg(\eta_i) = pg(\alpha)$. 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 pth powers successively to obtain

$$\begin{aligned}\bar{\eta}_i^{p^{\beta+e-2}} &= \alpha^{p^{\beta+e-2}} + p^{e-1}h(\alpha),\\ \bar{\eta}_i^{l+k} &= \bar{\eta}_i^{p^{\beta+e-2}\gamma+k} = \left(\alpha^{p^{\beta+e-2}} + p^{e-1}h(\alpha)\right)^\gamma \bar{\eta}_i^k\\ &= \left(\alpha^{p^{\beta+e-2}\gamma} + p^{e-1}h_1(\alpha)\right)\bar{\eta}_i^k.\end{aligned}$$

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

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

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

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

$$S_r^{n+1}\left(\bar{\eta}_1^k, \ldots, \bar{\eta}_{n+1}^k\right) \equiv 0 \bmod p,$$

and so

$$S_r^{n+1}\left(\bar{\eta}_1^{l+k}, \ldots, \bar{\eta}_{n+1}^{l+k}\right) \equiv S_r^{n+1}\left(\bar{\eta}_1^k, \ldots, \bar{\eta}_{n+1}^k\right) \bmod p^e.$$

7. Determination of the kernel of ψ

As shown in Section 6, there is a homomorphism ψ: $\mathbf{Z}_l^* \to G(n)$, where $\mathbf{Z}_l^*$ is the multiplicative group of reduced residues mod l, where l is defined in Theorem 3, and ψ is defined by

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

We assume $e \geqslant 2$, and since the case $n = 1$ was solved in [1], we assume $n \geqslant 2$. In the case $e = 1$, the kernel of ψ is non-trivial (see [9]) and if $e = 2$, $n = 1$, the kernel is $\{\pm 1\}$, as shown in [1]. For $n \geqslant 2$, $e \geqslant 2$, we shall show in this section that $\ker \psi = \{1\}$, and so ψ is an isomorphism.

LEMMA 2. *If* $k \in \ker \psi$, *then* $k \equiv 1 \bmod \gamma$, *where*

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

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

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

From Taylor's formula ([2], p. 268), if g_t denotes the t th component of $g(n, k)$, then

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

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

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

Replacing J by I_n in the identity $J \cdot [\partial u_l/\partial \sigma_i] = [\partial g_l/\partial \sigma_i]$, we obtain

$$\frac{\partial u_l}{\partial \sigma_i} = \frac{\partial g_l}{\partial \sigma_i}.$$

Taking $l = 1$, $\sigma_i - \sigma_{n+1} = k(\sigma_i^k - \sigma_{n+1}^k)$, 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 we have $p \nmid k$. If $p = 2$, this shows $k \equiv 1 \bmod p$. If $p \neq 2$, choose $\sigma_1 = -\sigma_2 = \sigma(\neq 0, \sigma \in \mathbf{Z}/(p))$. 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 $\mathbf{F}_{p^r}$, $2 \leqslant r \leqslant n$, and let $g(x)$ be its minimal polynomial over $\mathbf{F}_p$. 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 $\lambda^{-1} \in \mathbf{F}_p$. Thus $k \equiv 1 \bmod (p^r - 1)$, $1 \leqslant r \leqslant n$. 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

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

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

LEMMA 3. *If* $\beta = 1$, *then* $k \in \ker \psi$ *only if* $k \equiv 1 \bmod p^{e-1}$.

https://doi.org/10.1017/S1446788700024435 Published online by Cambridge University Press

PROOF. Let $f(x)$ have degree two, and constant term 1. We assume $n \geqslant 2$. Then $g(x) = (x-1)^{n-1}f(x)$ has degree $(n+1)$. If $k \in \ker \psi$, then $k \equiv \pm 1 \bmod p^{e-1}(\frac{p^2-1}{2})$, by [1], Theorem 3.6, p. 91, since p is odd $(n+1 \leqslant p)$. Since $k \equiv 1 \bmod (p^2-1)$ by Lemma 2, the positive sign holds, and so $k \equiv 1 \bmod p^{e-1}$.

LEMMA 4. *If $\beta \geqslant 2$ and $e = 2$ then $k \in \ker \psi$ only if $k \equiv 1 \bmod p^{\beta}$.*

PROOF. We construct a sequence $u_1, \ldots, u_n$ for which $\boldsymbol{g}(n,k)(u_1, \ldots, u_n) \neq \boldsymbol{g}(n,1)(u_1, \ldots, u_n)$ for $1 < k < p^{\beta}+1$. It is sufficient to do this for the first components of the vectors $\boldsymbol{g}(n,k)$, 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 $\deg g(x) < n$, 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

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

for $k < n$. This follows from the recurrence relation for the g_k's given in Lidl [7], p. 183. Choose $\lambda_1 \not\equiv 0 \bmod p$, and $\lambda_2, \ldots, \lambda_{n-1}$ in turn such that $g_k(u_1, \ldots, u_n) \equiv n+1 \bmod p^2$, $2 \leqslant k \leqslant n-1$. Since $p^{\beta-1} < n+1$, $n \geqslant p^{\beta-1}$. If $n > p^{\beta-1}$, choose λ_n in the same fashion. In this case, $g_k \neq g_1$ if $k < n$. In particular, this holds for $k = 1 + p^{\beta-1}$. If $n = p^{\beta-1}$, then $g_n = n+1$, 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

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

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

Now consider $f(x)$ of the form

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

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

$$g_k(u_1, \ldots, u_n) \neq g_1(u_1, \ldots, u_n), \quad \text{for } k < p^{\beta-1}.$$

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

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

Since $\ker \psi$ is a subgroup of $\mathbf{Z}_l^*$, if $k \in \ker \psi$ then $k^s \in \ker \psi$, which is false. Thus the condition $k \equiv 1 \bmod p^{\beta}$ is necessary if $e = 2$.

We note that Lemma 4 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

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

If $p|(n+1)$, take

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

LEMMA 5. *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 $\mathbf{Z}/(p^2)$.*

PROOF. For a fixed $(u_1, \ldots, u_n)$, $\{g_k\}$ is a linear recurring sequence. We apply results from Ward [13] to $\{g_k\}$. It should be noted that Theorem 7.1 of Ward's earlier paper [12] on sequences of length three, and Theorem 11.1 of [13], imply that the period of such a sequence mod p^N is $p^b\lambda$, where λ is the period mod p, and where $b \leqslant N$. 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 [13], p. 606, which states that the period of a linear recurring sequence mod p^e is the least integer t such that

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

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

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

Let $l \in \mathbf{Z}$. Then

$$(x^{p^l} - 1)f'(x) - (n+1)\left(\frac{x^{p^l}-1}{x-1}\right)f(x)$$
$$= p\left(\frac{x^{p^l}-1}{x-1}\right)\big[(x-1)g'(x) - (n+1)g(x)\big] = pk(x).$$

Modulo p, $(x-1)^{p^l-1}$ divides $k(x)$ if $p \nmid (n+1)$, and no higher power of $(x-1)$ does so, and if $p|(n+1)$, $k(x)$ is divisible by $(x-1)^{p^l}$ and no higher power. Thus $pk(x) \equiv 0 \bmod (p^2, f(x))$ if and only if $p^l - 1 \geqslant n+1$, or $p^l \geqslant n+2$, if $p \nmid (n+1)$, or $p^l \geqslant n+1$ if $p|(n+1)$. Thus the period of $\{g_k(u_1, \ldots, u_n)\} \bmod p^2$ is p^β, where $p^{\beta-1} < n+1 \leqslant p^\beta$.

https://doi.org/10.1017/S1446788700024435 Published online by Cambridge University Press

LEMMA 6. *The sequence* $\{g_k\}$ *of Lemma* 5 *has period* $p^{e+\beta-2}$ *over* $\mathbf{Z}/(p^e)$.

PROOF. It is known that $p^{\beta+1}$ is a period for $\{g_k\}$ with $e = 3$. Assume p^β is likewise. Since $\beta \geqslant 2$,

$$pk(x) = p\left(\frac{x^{p^\beta} - 1}{x^{p^{\beta-1}} - 1}\right)k_1(x),$$

where $k(x)$ is as in the proof of Lemma 5, and where $k_1(x)$ is divisible by $(x-1)^{p^{\beta-1}-1} \bmod p$ if $p \nmid (n+1)$ and by $(x-1)^{p^{\beta-1}}$ if $p|(n+1)$.

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 $s \geqslant 1$. If $x = 1$, $p = p\lambda(1)$, so $\lambda(1) \equiv 1 \bmod p$, and so $(x-1) \nmid \lambda(x) \bmod p$.

$$p\left(\frac{x^{p^\beta} - 1}{x^{p^{\beta-1}} - 1}\right)k_1(x) = p^2\lambda(x)k_1(x) \bmod (p^3, f(x)).$$

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 $f(x) = (x-1)^{n+1} \bmod p$, where $n + 1 > p^{\beta-1}$. Thus $\lambda(x)k_1(x) \not\equiv 0 \bmod (p, f(x))$, 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 $x^{p^\beta} - 1/(x^{p^{\beta-1}} - 1) = (x-1)^{p^\beta - p^{\beta-1}} + p\lambda(x)$, $\lambda(x) \in \mathbf{Z}[x]$, and $(x-1) \nmid \lambda(x) \bmod p$. If $s = (n+1) - (p^\beta - p^{\beta-1})$, then $s \geqslant 1$, 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 $\bmod p$, 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 $\bmod (p^3, f(x))$.

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 $\deg g(x) \geqslant 2$, or $n + 1 \geqslant 3$, 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 to $e > 3$, multiply in turn by expressions of the form $(x^{p^{l+1}} - 1)/(x^{p^l} - 1)$, where $l \geqslant \beta$. As in Case 1, this is equal to $p\lambda(x) \bmod f(x)$

where $(x-1)\mid\lambda(x) \bmod p$. 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 $n+1 \leqslant p^\beta$, then choose $g(x)$ as in Case 3. The corresponding expression is

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

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.

THEOREM 4. *If $e \geqslant 2$ and $n > 1$ then the group $G(n, p^e)$ of permutations of $(\mathbf{Z}/(p^e))^n$ induced by polynomial vectors of the form $\mathbf{g}(n, k)$ is isomorphic to the multiplicative group of reduced residues* mod *l, where $l = p^{e+\beta-2}\gamma$, $p^{\beta-1} < n+1 \leqslant p^\beta$, and $\gamma = \operatorname{lcm}(p-1, \ldots, p^n - 1, (p^{n+1}-1)/(p-1))$.*

PROOF. By Theorem 3, the mapping $\psi\colon \mathbf{Z}_l^* \to G(n, p^e)$ is a surjective homomorphism. We show that $\ker\psi = \{1\}$. By Lemma 2, if $k \in \ker\psi$, 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 3, and from Lemma 4 if $\beta \geqslant 2$ and $e = 2$. If $\beta \geqslant 2$, $e > 2$, proceed by induction on e. If $k \equiv 1 \bmod p^{e+\beta-2}$ is a necessary condition for $k \in \ker\psi \bmod p^e$, then $\bmod p^{e+1}$, the same condition is necessary for $k \in \ker\psi'$, where ψ' corresponds to $\psi \bmod p^{e+1}$. Thus $k \equiv 1 + tp^{e+\beta-2} \bmod p^{e+\beta-1}$. We show that $t \equiv 0 \bmod p$. If there exists $k \in \ker\psi'$ 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 $k' = 1 + p^{e+\beta-2} \in \ker\psi'$, and so

$$k'^t \in \ker\psi' \quad \text{for all } t \in \mathbf{Z}.$$

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 $G(n, p^e) \simeq \mathbf{Z}_l^*$, and so there exists an isomorphism $\phi\colon \mathbf{Z}_l^* \to G(n, p^{e+1})$. Thus if $\alpha, \beta \in \mathbf{Z}$, $\alpha \equiv \beta \bmod l$, then $\mathbf{g}(n, \alpha)$ and $\mathbf{g}(n, \beta)$ induce the same map. By Lemma 6, there is a sequence $\{g_k\}$ with period $p^{e+\beta-1}$ over $\mathbf{Z}/(p^{e+1})$. 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.

8. The general case: $R = \mathbf{Z}/(m)$

We assume $n \geqslant 2$. For $n = 1$ see [1], Section 6. Let $m = \prod_{i=1}^r p_i^{\alpha_i}$ be the prime decomposition of m over $\mathbf{Z}$, and let $G(n, m)$ be the group of permutations of R induced by $\{\mathbf{g}(n, k)\colon k \in \mathbf{Z}\}$. Let

$$\lambda_i = \operatorname{lcm}\big(p_i - 1, \ldots, p_i^n - 1, (p_i^{n+1}-1)/(p_i - 1)\big).$$

If $\alpha_i = 1$, set $\mu_i = \lambda_i$. If $\alpha_i > 1$, set

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

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

LEMMA 7. *If $k \equiv l \bmod L$, then the maps of R^n induced by $\mathbf{g}(n, k)$ and $\mathbf{g}(n, l)$ are equal.*

PROOF. If $k \equiv l \bmod L$ then $k \equiv l \bmod \mu_i$, $1 \leqslant i \leqslant r$. Thus by Theorem 3 (in the case $\alpha_i \geqslant 2$) and by the corollary to Theorem 4 of [9] (in the case $\alpha_i = 1$), $\mathbf{g}(n, k)$ and $\mathbf{g}(n, l)$ induce the same map on R_i^n, where $R_i = \mathbf{Z}/(p_i^{\alpha_i})$. By the Chinese remainder theorem, $R \simeq \prod_{i=1}^r R_i$, and so $\mathbf{g}(n, k)$ and $\mathbf{g}(n, l)$ induce the same map on R^n.

LEMMA 8. *The map $\psi\colon \mathbf{Z}_L^* \to G(n, m)$ defined by $\psi(k) \mapsto \{$map of R^n induced by $\mathbf{g}(n, k)\}$ is a homomorphism.*

PROOF. $\mathbf{g}(n, k)$ is a permutation polynomial vector over $\mathbf{Z}/(m)$ if and only if $(k, L) = 1$. The rest follows from Lemma 7.

LEMMA 9. *The kernel of ψ, where ψ is defined in Lemma* 8, *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 $k \in \ker\psi$, then $\mathbf{g}(n, k)$ induces the identity map on $\mathbf{Z}/(p_i^{\alpha_i})$, $1 \leqslant i \leqslant r$. If $\alpha_i \geqslant 2$, 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 of [9]. The map $k \bmod L \to (k \bmod \mu_1, \ldots, k \bmod \mu_r)$ is a monomorphism of $\ker\psi$ into $\prod_{i=1}^r \ker\psi_i$, where $\psi_i = \psi|_{R_i}$ and $R_i = \mathbf{Z}/(p_i^{\alpha_i})$, and the result follows.

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

THEOREM 5. *If $m = \prod_{i=1}^r p_i^{\alpha_i}$ and $\alpha_i \geqslant 2$ for $1 \leqslant i \leqslant r$, and $n \geqslant 2$ then $G(n, m)$, the group of permutations of $R^n = (\mathbf{Z}/(m))^n$ induced by $\{\mathbf{g}(n, k)\}$ is isomorphic to the multiplicative group of reduced residues* mod L, *where*

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

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

and

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

https://doi.org/10.1017/S1446788700024435 Published online by Cambridge University Press

References

[1] 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), 88–99.

[2] H. Lausch and W. Nöbauer, *Algebra of polynomials* (North-Holland, Amsterdam, 1973).

[3] R. Lidl and C. Wells, 'Chebyshev polynomials in several variables', *J. reine angew. Math.* **273** (1972), 178–198.

[4] R. Lidl, 'Tschebyscheffpolynome und die dadurch dargestellten Gruppen,' *Monatsh. Math.* **77** (1973), 132–147.

[5] _____, 'Über die Struktur einer durch Tschebyscheffpolynome in 2 Variablen dargestellten Permutationsgruppe,' *Beiträge Algebra Geometrie* **3** (1974), 41–48.

[6] _____, 'Reguläre Polynome über endlichen Körpern,' *Beiträge Algebra Geometrie* **2** (1974), 58–59.

[7] _____, 'Tschebyscheffpolynome in mehreren Variablen,' *J. reine angew. Math.* **273** (1975), 178–198.

[8] B. McDonald, *Finite rings with identity* (Dekker, New York, 1974).

[9] R. Matthews, '*Some generalisations of Chebyshev polynomials and their induced group structure over a finite field*', *Acta Arithmetica*, to appear.

[10] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers* (Polish Scientific Publishers, Warsaw, 1974).

[11] W. Nöbauer, 'Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen', *J. reine angew. Math.* **231** (1968), 215–219.

[12] M. Ward, 'The characteristic number of a sequence of integers satisfying a linear recursion relation', *Trans. Amer. Math. Soc.* **33** (1931), 153–165.

[13] _____, 'The arithmetical theory of linear recurring series', *Trans. Amer. Math. Soc.* **35** (1933), 600–628.

Department of Mathematics
University of Tasmania
Hobart, Tasmania
Australia