J. Austral. Math. Soc. (*Series A*) 27 (1979), 232–238

LOCAL POLYNOMIAL FUNCTIONS ON FACTOR RINGS OF THE INTEGERS

HANS LAUSCH and WILFRIED NÖBAUER

(Received 31 May 1978)

Communicated by R. Lidl

Abstract

Let A be a universal algebra. A function $\varphi: A^k \to A$ is called a t-local polynomial function, if φ can be interpolated on any t places of A^k by a polynomial function—for the definition of a polynomial function on A, see Lausch and Nöbauer (1973). Let $P_k(A)$ be the set of all polynomial functions, $L_t P_k(A)$ the set of all t-local polynomial functions on A and $LP_k(A)$ the intersection of all $L_t P_k(A)$, then

$$L_1 P_k(A) \supseteq L_2 P_k(A) \supseteq \ldots \supseteq LP_k(A) \supseteq P_k(A).$$

If A is an abelian group, then this chain has at most five distinct members—see Hule and Nöbauer (1977)—and if A is a lattice, then it has at most three distinct members—see Dorninger and Nöbauer (1978). In this paper we show that in the case of commutative rings with identity there does not exist such a bound on the length of the chain and that, in this case, there exist chains of even infinite length.

Subject classification (*Amer. Math. Soc.* (*MOS*) *1970*): 08 A 25 (13 B 25).

1

Let R be a commutative ring with identity. $L_n P_1(R)$ denotes the set of all maps φ from R to R such that, for any n (not necessarily distinct) elements $x_1, \ldots, x_n \in R$, there exists a polynomial $\pi(x) \in R[x]$ such that $\varphi(x_1) = \pi(x_1)$, for $i = 1, 2, \ldots, n$. Furthermore, $LP_1(R)$ will denote the intersection of all $L_n P_1(R)$, $n = 1, 2, \ldots$, and $P_1(R)$ the set of all maps φ from R to R such that there exists a polynomial $\pi(x) \in R[x]$ with $\varphi(r) = \pi(r)$ for all $r \in R$. Then we have the descending chain

$$L_1 P_1(R) \supseteq L_2 P_1(R) \supseteq L_3 P_1(R) \supseteq \ldots \supseteq LP_1(R) \supseteq P_1(R).$$

The question arises which links of this chain reduce to equalities. Two types of

This paper was written while the first author was visiting professor at the Technische Universität Wien, Austria.

rings will be studied: $R = \mathbf{Z}$ and $R = \mathbf{Z}/(n)$, $n > 0$ an integer. By Corollary 1 of Dorninger and Nöbauer (1978) it is sufficient, in the latter case, to study only the case where $n = p^e$, p being a prime, $e > 0$ an integer. For $e = 1$ it is well known that $L_1 P_1(\mathbf{Z}/(p)) = P_1(\mathbf{Z}/(p))$, and it is obviously true for any e that

$$LP_1(\mathbf{Z}/(p^e)) = P_1(\mathbf{Z}/(p^e)).$$

For $e > 1$ we need the following theorem which follows easily from a theorem by Nöbauer (1955).

THEOREM 1. *Let* $\varepsilon(k) = max\{s | s \geqslant 0,\ s \in \mathbf{Z}, p^s | k!\}$. *Any map* $\varphi \in P_1(\mathbf{Z}/(p^e))$ *is of the following form*:

$$\varphi\colon a + px \to c_{0a} + pc_{1a}x + p^2 c_{2a} x(x-1) + \ldots + p^{e-1} c_{e-1a} x(x-1)\ldots(x-e+2),$$

where $a = 0, 1, \ldots, p-1$, $x = 0, 1, \ldots, p^{e-1} - 1$, *and where* c_{ka} *may be any integer with* $0 \leqslant c_{ka} \leqslant p^{max(0, e-k-\varepsilon(k))} - 1$ *for* $k = 0, 1, \ldots, e-1$. *Conversely, any such map belongs to* $P_1(\mathbf{Z}/(p^e))$.

THEOREM 2. *Let* $e > 1$ *be an integer and* $f > 0$ *an integer such that* $f + \varepsilon(f) \leqslant e$. *Then* $L_f(\mathbf{Z}/(p^e)) \supset L_{f+1}(\mathbf{Z}/(p^e))$.

PROOF. Let $\varphi\colon \mathbf{Z}/(p^e) \to \mathbf{Z}/(p^e)$ be the map defined by

$$\varphi(a + px) = p^{f-1} x(x-1)\ldots(x-(f-1))$$

for all $a = 0, 1, \ldots, p-1$ and all $x = 0, \ldots, p^{e-1} - 1$. If $x_1, \ldots, x_f$ are any f integers between 0 and $p^{e-1} - 1$, then the map $\pi\colon \mathbf{Z}/(p^e) \to \mathbf{Z}/(p^e)$ defined by

$$\pi(a + px) = p^{f-1}[x(x-1)\ldots(x-(f-1)) - (x-x_1)\ldots(x-x_f)]$$

is, by Theorem 1, an element of $P_1(\mathbf{Z}/(p^e))$ and $\varphi(a + px_i) = \pi(a + px_i)$ for $i = 1, \ldots, f$, and hence we conclude that $\varphi \in L_f P_1(\mathbf{Z}/(p^e))$. Now we are going to show that $\varphi \notin L_{f+1} P_1(\mathbf{Z}/(p^e))$. Assume the opposite is true; then for any $a = 0, 1, \ldots, p-1$, there exists, by Theorem 1, a polynomial

$$\chi(x) = c_{0a} + pc_{1a}x + \ldots + p^r c_{ra} x(x-1)\ldots(x-(r-1)), \quad c_{ra} \not\equiv 0 \bmod p^{e-r-\varepsilon(r)},$$

such that $\chi(k) = \varphi(a + pk)$, for $k = 0, 1, \ldots, f$. If $r < f$, then the substitution of $0, 1, \ldots, r$ for k shows that $p^r c_{ra} r! \equiv 0 \bmod p^e$ whence $c_{ra} \equiv 0 \bmod p^{e-r-\varepsilon(r)}$, a contradiction. If $r \geqslant f$, then substitution of $0, 1, \ldots, f$ for k leads to

$$p^{f-1+\varepsilon(f)}(pc_{fa} - 1) \equiv 0 \bmod p^e$$

whence $f - 1 + \varepsilon(f) \geqslant e \geqslant f + \varepsilon(f)$, a contradiction.

THEOREM 3. *Let* $e > 1$ *be an integer and* $f > 0$ *the smallest integer such that* $f + \varepsilon(f) \geqslant e$. *Then* $L_{f+1} P_1(\mathbf{Z}/(p^e)) = P_1(\mathbf{Z}/(p^e))$.

https://doi.org/10.1017/S1446788700012155 Published online by Cambridge University Press

PROOF. Let $\varphi \in L_{f+1}(P_1(\mathbf{Z}/(p^e)))$. Put $f-1=r$; then $r+\varepsilon(r)<e$. For each a, $0 \leqslant a < p$, there exist $a_0, a_1, \ldots, a_r \in \mathbf{Z}$, $0 \leqslant a_k \leqslant p^{e-k-\varepsilon(k)}-1$, by Theorem 1, such that

$$\varphi(a+px) = a_0 + pa_1 x + p^2 a_2 x(x-1) + \ldots + p^r a_r x(x-1)\ldots(x-r+1)$$

$$\text{for } x = 0, 1, \ldots, r,$$

since $r+1<f+1$ and therefore $\varphi \in L_{r+1} P_1(\mathbf{Z}/(p^e))$. But substitution of $x = 0, 1, \ldots, r$ determines a_k for $k = 0, \ldots, r$. Since $\varphi \in L_{r+2} P_1(\mathbf{Z}/(p^e))$, interpolation at $0, 1, 2, \ldots, r, x$ shows that for any x,

$$\varphi(a+px) = a_0 + pa_1 x + p^2 a_2 x(x-1) + \ldots + p^r a_r x(x-1)\ldots(x-(r-1)).$$

From Theorem 1, we now conclude, that $\varphi \in P_1(\mathbf{Z}/(p^e))$ and hence

$$L_{f+1} P_1(\mathbf{Z}/(p^e)) = P_1(\mathbf{Z}/(p^e)).$$

In order to complete the investigation about the interpolation over $\mathbf{Z}/(p^e)$, we are left with the case where, if f is defined as in Theorem 3, $f+\varepsilon(f)>e$. The following theorem will settle this problem.

THEOREM 4. *Let $e>1$, $r>0$ be integers with $r+\varepsilon(r)<e$ and $(r+1)+\varepsilon(r+1)>e$. Then $L_{r+1} P_1(\mathbf{Z}/(p^e)) = P_1(\mathbf{Z}/(p^e))$.*

PROOF. Let $\varphi \in L_{r+1} P_1(\mathbf{Z}/(p^e))$. Then for each a with $0 \leqslant a < p$, there exists a polynomial $\pi(x) = a_0 + pa_1 x + p^2 a_2 x(x-1) + \ldots + p^r a_r x(x-1)\ldots(x-r+1)$, by Theorem 1, such that $\varphi(a+px) = \pi(x)$ for $x = 0, 1, \ldots, r$. There, $a_0, pa_1, \ldots, p^{r-1} a_{r-1}$ are determined by $\varphi(a), \varphi(a+p), \ldots, \varphi(a+(r-1)p)$. Furthermore, there exists a polynomial $\rho(x)$ of the form of Theorem 1 such that $\varphi(a+px) = \rho(x)$, for $x = 0, 1, \ldots, r-1, r+1$ and hence $\rho(x)$ is of the form

$$\rho(x) = a_0 + pa_1 x + p^2 a_2 x(x-1) + \ldots + p^{r-1} a_{r-1} x(x-1)\ldots(x-r+2)$$

$$+ p^r \bar{a}_r x(x-1)\ldots(x-r+1).$$

But $p^r \bar{a}_r (r+1)! \equiv 0 \bmod p^e$ since $r+\varepsilon(r+1) \geqslant e$, and $p^r a_r (r+1)! \equiv 0 \bmod p^e$ for the same reason. Hence $\varphi(a+px) = \pi(x)$ for $x = 0, 1, \ldots, r, r+1$. Let us now rewrite $\pi(x)$ in the form

$$\pi(x) = b_0 + pb_1(x-1) + p^2 b_2(x-1)(x-2) + \ldots + p^r b_r(x-1)(x-2)\ldots(x-r).$$

We note again that $b_0, pb_1, \ldots, p^{r-1} b_{r-1}$ are determined by

$$\varphi(a+p), \varphi(a+2p), \ldots, \varphi(a+rp).$$

Furthermore, there exists a polynomial

$$\sigma(x) = b_0 + pb_1(x-1) + \ldots + p^{r-1} b_{r-1}(x-1)\ldots(x-r+1) + p^r \bar{b}_r(x-1)\ldots(x-r)$$

such that $\varphi(a+px) = \sigma(x)$ for $x = 1, 2, \ldots, r, r+2$. But $p^r \bar{b}_r (r+1)! \equiv 0 \bmod p^e$ and $p^r b_r (r+1)! \equiv 0 \bmod p^e$ and hence $\varphi(a+px) = \pi(x)$, for $x = 0, 1, \ldots, r, r+1, r+2$.

This procedure can be continued until we obtain $\varphi(a+px) = \pi(x)$, for all x, that is $\varphi \in P_1(\mathbf{Z}/(p^e))$.

2

Now we turn our attention to $\mathbf{Z}$. Let $\varphi\colon \mathbf{Z}\to\mathbf{Z}$ be a map and

$$\Delta\varphi(x,y) = (\varphi(x)-\varphi(y))(x-y)^{-1}, \quad x\neq y,$$

the difference quotient of φ. We need two lemmas:

LEMMA 5. *Let $\varphi\colon \mathbf{Z}\to\mathbf{Z}$ be a map. Then $\varphi \in L_n P_1(\mathbf{Z})$ if and only if, for all $y\in\mathbf{Z}$ and any $n-1$ integers $x_1,\dots,x_{n-1}$ which are distinct from y, there exists $\rho_y \in P_1(\mathbf{Z})$ such that*

$$\Delta\varphi(x_i,y) = \rho_y(x_i), \quad i = 1,\dots,n-1.$$

PROOF. (i) Let $\varphi \in L_n P_1(\mathbf{Z})$, $y\in\mathbf{Z}$, and $x_1,\dots,x_{n-1}$ be integers distinct from $\mathbf{Z}$. Then $\varphi(x_i) = \varphi(y)+\Delta\varphi(x_i,y)(x_i-y)$, $i = 1,\dots,n-1$. By assumption, there exists $\pi\in P_1(\mathbf{Z})$ such that $\varphi(x_i) = \pi(x_i)$, $i = 1,\dots,n-1$, and $\varphi(y) = \pi(y)$. Therefore $\pi(x_i) = \pi(y)+\Delta\varphi(x_i,y)(x_i-y)$. On the other hand, $\pi(x_i) = \pi(y)+\Delta\pi(x_i,y)(x_i-y)$, $i = 1,\dots,n-1$. As $x_i \neq y$, we have

$$\Delta\varphi(x_i,y) = \Delta\pi(x_i,y), \quad i = 1,\dots,n-1.$$

If $p(u)\in Z[u]$ is such that $p(x) = \pi(x)$, for all $x\in\mathbf{Z}$, then

$$r(u,v) = (p(u)-p(v))(u-v)^{-1}\in\mathbf{Z}[u,v],$$

and

$$\Delta\pi(x_i,y) = r(x_i,y).$$

Put $\rho_y(x) = r(x,y)$ to obtain the desired result.

(ii) Let $\Delta\varphi(x,y)$ satisfy the conditions of the lemma, and let $x_1,\dots,x_n$ be n distinct integers. Then there exists $\rho_{x_n}\in P_1(\mathbf{Z})$ such that $\Delta\varphi(x_i,x_n) = \rho_{x_n}(x_i)$, $i = 1,\dots,n-1$. Then

$$\begin{aligned}\varphi(x_i) &= \varphi(x_n)+\Delta\varphi(x_i,x_n)(x_i-x_n)\\ &= \varphi(x_n)+\rho_{x_n}(x_i)(x_i-x_n).\end{aligned}$$

Let $\pi(x) = \varphi(x_n)+\rho_{x_n}(x)(x-x_n)$; then $\pi\in P_1(\mathbf{Z})$. Moreover,

$$\pi(x_i) = \varphi(x_n)+\rho_{x_n}(x_i)(x_i-x_n) = \varphi(x_i)$$

and

$$\pi(x_n) = \varphi(x_n).$$

Therefore $\varphi\in L_n P_1(\mathbf{Z})$.

https://doi.org/10.1017/S1446788700012155 Published online by Cambridge University Press

LEMMA 6. *Let* $\varphi_n(x) = \frac{1}{2}(x-1)\dots(x-n)$. *Then for all* $y \in \mathbf{Z} \setminus \{x\}$ *and* $n \geqslant 3$, *there exists* $\pi_{y,n} \in P_1(\mathbf{Z})$ *such that*

$$\Delta\varphi_n(x,y) = \varphi_{n-1}(x) + (y-n)\,\varphi_{n-2}(x) + \pi_{y,n}(x).$$

PROOF. Proof is by induction on n. (i) Putting $n = 3$, $\varphi_3(x) = \frac{1}{2}(x-1)(x-2)(x-3)$ and hence

$$\begin{aligned}
\Delta\varphi_2(x,y) &= \frac{1}{2(x-y)}[(x-1)(x-2)(x-3) - (y-1)(y-2)(y-3)] \\
&= \frac{1}{2(x-y)}[(x-1)(x-2)((x-y)+(y-3)) - (y-1)(y-2)(y-3)] \\
&= \varphi_2(x) + \frac{1}{2}\frac{y-3}{x-y}[(x-1)(x-2) - (y-1)(y-2)] \\
&= \varphi_2(x) + (y-3)\,\varphi_1(x) + \frac{(y-3)(y-2)}{2} \\
&= \varphi_2(x) + (y-3)\,\varphi_1(x) + \pi_{y,3}(x) \quad \text{where } \pi_{y,3}(x) = \frac{(y-3)(y-2)}{2} \in \mathbf{Z}.
\end{aligned}$$

(ii) Suppose the lemma has been proved for $n-1$, $n \geqslant 4$. Then by a similar argument as for $n = 3$, one obtains

$$\Delta\varphi_n(x,y) = \varphi_{n-1}(x) + (y-n)\,\varphi_{n-2}(x) + \pi_{y,n}(x),$$

where

$$\pi_{y,n}(x) = (y-n)\,\pi_{y,n-1}(x) + \frac{(y-n)(y-n+1)}{2}(x-1)\dots(x-n+3)$$

and hence $\pi_{y,n} \in P_1(\mathbf{Z})$.

THEOREM 7. *For* $n \geqslant 1$ *and* φ_n *as in Lemma* 6, *the following holds*:

$$\varphi_{2n}, \varphi_{2n+1} \in L_n P_1(\mathbf{Z}) \setminus L_{n+1} P_1(\mathbf{Z}).$$

In particular,

$$L_1 P_1(\mathbf{Z}) \supset L_2 P_1(\mathbf{Z}) \supset \dots \supset L_n P_1(\mathbf{Z}) \supset L_{n+1} P_1(\mathbf{Z}) \supset \dots \supset L P_1(\mathbf{Z}).$$

PROOF. Proof is by induction on n. (i) Putting $n = 1$, $\varphi_2(x) = \frac{1}{2}(x-1)(x-2)$, $\Delta\varphi_2(3,1) = \frac{1}{2}$ and hence by Lemma 5, $\varphi_2 \notin L_2 P_1(\mathbf{Z})$ but $\varphi_2 \in L_1 P_1(\mathbf{Z})$, $\varphi_3(x) = \frac{1}{2}(x-1)(x-2)(x-3)$, $\Delta\varphi_3(4,2) = \frac{3}{2}$ and hence again by Lemma 5, $\varphi_3 \notin L_2 P_1(\mathbf{Z})$ but $\varphi_3 \in L_1 P_1(\mathbf{Z})$.

(ii) Suppose $n \geqslant 2$, and $\varphi_{2n-2}, \varphi_{2n-1} \in L_{n-1} P_1(\mathbf{Z}) \setminus L_n P_1(\mathbf{Z})$. By Lemma 6, for all $x \neq y$, we have

$$\Delta\varphi_{2n}(x,y) = \varphi_{2n-1}(x) + (y-2n)\,\varphi_{2n-2}(x) + \pi_{y,2n}(x), \quad \text{with } \pi_{y,2n} \in P_1(\mathbf{Z}).$$

https://doi.org/10.1017/S1446788700012155 Published online by Cambridge University Press

Let $x_1, \ldots, x_{n-1} \in \mathbf{Z}$ and y be an integer distinct from $x_1, \ldots, x_{n-1}$. By induction, there exists $\rho_y \in P_1(\mathbf{Z})$ such that $\Delta\varphi_{2n}(x_i, y) = \rho_y(x_i)$, $i = 1, \ldots, n-1$. By Lemma 5, $\varphi_{2n} \in L_n P_1(\mathbf{Z})$.

Suppose $\varphi_{2n} \in L_{n+1} P_1(\mathbf{Z})$. Then there exist integers $a_0, a_1, a_2, \ldots$ such that

$$\varphi_{2n}(2k) = a_0 + a_1(2k-2) + a_2(2k-2)(2k-4) + \ldots \quad \text{for } k = 1, 2, \ldots, n+1.$$

But $\varphi_{2n}(2k) = 0$, for $k = 1, \ldots, n$, and $\varphi_{2n}(2n+2) = \frac{1}{2}(2n+1)!$ This implies $a_0 = a_1 = \ldots = a_{n-1} = 0$, and $a_n . 2n . (2n-2) \ldots 4 . 2 = \frac{1}{2}(2n+1)!$ Hence

$$a_n = \tfrac{1}{2}(2n+1)(2n-1) \ldots 3..1 \notin \mathbf{Z}$$

which is a contradiction. Therefore $\varphi_{2n} \notin L_{n+1} P_1(\mathbf{Z})$.

By Lemma 6, for all $x \neq y$, we have

$$\Delta\varphi_{2n+1}(x, y) = \varphi_{2n}(x) + (y - 2n - 1)\varphi_{2n-1}(x) + \pi_{y, 2n+1}(x) \quad \text{with } \pi_{y, 2n+1} \in P_1(\mathbf{Z}).$$

Let $x_1, \ldots, x_{n-1} \in \mathbf{Z}$ and y be an integer distinct from $x_1, \ldots, x_{n-1}$. By induction and by the first part of this proof there exists $\rho_y \in P_1(\mathbf{Z})$ such that

$$\Delta\varphi_{2n+1}(x_i, y) = \rho_y(x_i), \quad i = 1, \ldots, n-1.$$

By Lemma 5, $\varphi_{2n+1} \in L_n P_1(\mathbf{Z})$. Suppose $\varphi_{2n+1} \in L_{n+1} P_1(\mathbf{Z})$. Then there exist integers $a_0, a_1, a_2, \ldots$ such that $\varphi_{2n+1}(2k) = a_0 + a_1(2k-2) + a_2(2k-2)(2k-4) + \ldots$, for $k = 1, \ldots, n+1$. But $\varphi_{2n+1}(2k) = 0$, for $k = 1, \ldots, n$ and $\varphi_{2n+1}(2n+2) = \frac{1}{2}(2n+1)!$ This implies $a_0 = a_1 = \ldots a_{n-1} = 0$ and $a_n . 2n . (2n-2) \ldots 4 . 2 = \frac{1}{2}(2n+1)!$ Hence $a_n = \frac{1}{2}(2n+1)(2n-1) \ldots 3..1 \notin \mathbf{Z}$ which is a contradiction. Therefore

$$\varphi_{2n+1} \notin L_{n+1} P_1(\mathbf{Z}).$$

Finally we consider $LP_1(\mathbf{Z})$ in relation to $P_1(\mathbf{Z})$:

THEOREM 8. *Let $c, a_0, a_1, a_{-1}, a_2, a_{-2}, \ldots$ be a sequence in $\mathbf{Z}$. Then*

(i) $\varphi: x \to c + a_0 x + a_1 x(x-1) + a_{-1} x(x-1)(x+1) +$

$$\ldots + a_n x(x-1)(x+1) \ldots (x-n) + a_{-n} x(x-1)(x+1) \ldots (x-n)(x+n) + \ldots$$

belongs to $LP_1(\mathbf{Z})$.

(ii) *Pairwise distinct sequences give rise to pairwise distinct elements of $LP_1(\mathbf{Z})$.*

(iii) $LP_1(\mathbf{Z}) \supset P_1(\mathbf{Z})$.

PROOF.

(i) Let $x_1, \ldots, x_n \in \mathbf{Z}$. Then all but finitely many terms in the series contain all linear factors $x - x_1, \ldots, x - x_n$. Hence $\varphi(x_i) = \pi(x_i)$, for some $\pi \in P_1(\mathbf{Z})$ and $i = 1, \ldots, n$.

(ii) It suffices to show that if $c + a_0 x + a_1 x(x-1) + \ldots = 0$ for all $x \in \mathbf{Z}$, then

https://doi.org/10.1017/S1446788700012155 Published online by Cambridge University Press

$c = a_0 = a_1 = \ldots = 0$. But this follows when we substitute $0, 1, -1, 2, -2, \ldots$ into the left-hand side.

(iii) There are only countably many elements in $P_1(\mathbf{Z})$ but uncountably many sequences in $\mathbf{Z}$ whence (ii) implies the result.

References

D. Dorninger and W. Nöbauer (1978), 'Local polynomial functions on lattices and universal algebras', *Colloq. Math.* (to appear).

H. Hule and W. Nöbauer (1977), 'Local polynomial functions on universal algebras', *An. Acad. Brasil. Ciênc.* **49**(3), 365–372.

H. Lausch and W. Nöbauer (1973), *Algebra of polynomials* (North Holland, Amsterdam and London).

W. Nöbauer (1955), 'Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen', *Monatsh. Math.* **59**, 194–202.

Department of Mathematics
Monash University
Clayton, Vic. 3168
Australia

Institut für Algebra und
Mathematische Strukturtheorie
Technische Universität
Argentinierstrasse 8
A-1040 Wien
Austria