Riv. Mat. Univ. Parma (5) **6** (1997), 169-177

ERHARD AICHINGER (*)

Local polynomial functions on the integers (**)

1 - Introduction

We write $\mathbf{N}$ for the natural numbers, $\mathbf{N}_0$ for the naturals with 0, $\mathbf{Z}$ for the set of all integers, and $\boldsymbol{I}$ for the ring of integers $\langle \mathbf{Z}; +, \cdot \rangle$. For any algebra $\boldsymbol{A}$, we take $\mathsf{P}(\boldsymbol{A})$ to be the set of all unary polynomial functions on $\boldsymbol{A}$ (cf. [4]).

Let G and H be sets, let F be a subset of H^G, and let n be a natural number. We define $\mathsf{L}_n F$ as the set of all those functions from G to H that can be interpolated by a function in F at every subset of G with no more than n elements. Formally, this reads as

$$\mathsf{L}_n F = \{l\colon G \to H \mid \forall S \subseteq G\colon |S| \leq n \Rightarrow \exists f \in F \mid \forall \sigma \in S\colon f(\sigma) = l(\sigma)\}.$$

Furthermore, we put $\mathsf{L}F = \bigcap_{n \in \mathbf{N}} \mathsf{L}_n F$. For $F = \mathsf{P}(\boldsymbol{I})$, we obtain the chain of local polynomial functions on the integers, which has been investigated in [5]. In that paper, the following results about the chain $\mathsf{L}_n \mathsf{P}(\boldsymbol{I})$, $n \in \boldsymbol{N}$, have been proved:

1. For all $n \in \mathbf{N}$, the set $\mathsf{L}_{n+1} \mathsf{P}(\boldsymbol{I})$ is a proper subset of $\mathsf{L}_n \mathsf{P}(\boldsymbol{I})$. Actually, in [5] it is shown that for $\varphi_n(x) = \frac{1}{2}(x-1)(x-2)\ldots(x-n)$ we have $\varphi_{2n} \in \mathsf{L}_n \mathsf{P}(\boldsymbol{I})$ and $\varphi_{2n} \notin \mathsf{L}_{n+1} \mathsf{P}(\boldsymbol{I})$.

2. $\mathsf{LP}(\boldsymbol{I})$ is uncountable. This is shown by giving an explicit description of the functions that lie in $\mathsf{LP}(\boldsymbol{I})$.

(*) Institut für Algebra, Stochastik und wissensbasierte math. Systeme, J. Kepler Univ., Linz, Austria.

(**) Received December 19, 1997. AMS classification 08A40. Supported by a Doktorandenstipendium of the Austrian Academy of Sciences.

It will follow from our characterization that φ_{2n} is the *simplest possible* example of a function in $\mathsf{L}_n\mathsf{P}(\boldsymbol{I})$ that does not lie in $\mathsf{L}_{n+1}\mathsf{P}(\boldsymbol{I})$.

In [7] and [1], all functions from $\mathbf{N}$ to $\mathbf{Z}$ where $x-y$ divides $f(x)-f(y)$ for all $x, y \in \mathbf{N}$ are determined. Their result can easily be modified to obtain the set $\mathsf{L}_2\mathsf{P}(\boldsymbol{I})$. This set deserves special interest because it is the set of all congruence preserving functions on the ring of integers. On any algebra $\boldsymbol{A}$, we call a function c *congruence preserving* if $c(x)$ and $c(y)$ are congruent modulo the smallest congruence that collapses x and y. In the case of the ring of integers, this means that $c(x)-c(y)$ is a multiple of $x-y$ for all integers x and y.

2 - The characterization of $\mathsf{L}_n\mathsf{P}(\boldsymbol{I})$

We need the following definitions.

Definition 1. For all $n, i \in \mathbf{N}_0$ we define a natural number $A(n, i)$ by:

$$\begin{aligned} A(n, 0) &= 1 \quad \text{for all } n \in \mathbf{N}_0 \\ A(0, i) &= 1 \quad \text{for all } i \in \mathbf{N}_0 \\ A(n, i) &= \operatorname{lcm}(iA(n-1, i-1), A(n, i-1)) \quad \text{for all } n, i \in \mathbf{N}. \end{aligned}$$

From the recursive definition, we see that $A(n, i)$ is the least common multiple of all products that are formed by multiplying at most n different elements lying in $\{1, 2, \ldots, i\}$. For example,

$$\begin{aligned} &A(2, 5) \\ &\quad = \operatorname{lcm}(1, 2, 3, 4, 5, 1\cdot 2, 1\cdot 3, 1\cdot 4, 1\cdot 5, 2\cdot 3, 2\cdot 4, 2\cdot 5, 3\cdot 4, 3\cdot 5, 4\cdot 5) = 120. \end{aligned}$$

We are now ready to give the main results of the present note:

Proposition 1. *Let $n \in \mathbf{N}$, and let f be a function from $\mathbf{N}$ to $\mathbf{Z}$. Then the following statements are equivalent:*

1. *For all subsets S of $\mathbf{N}$ with at most n elements there exists a function p in $\mathsf{P}(\boldsymbol{I})$ such that $p|_S = f|_S$.*

2. *The function f can be written as*

$$f(x) = \sum_{i=0}^{\infty} c_i A(n-1, i)\binom{x-1}{i}$$

where $(c_i)_{i \in \mathbf{N}_0}$ is a sequence of integers.

For $n = 2$, this is precisely the result in [7]. We omit the proof of this result because it runs exactly as the proof of the following theorem, which gives a characterization of $\mathsf{L}_n \mathsf{P}(\boldsymbol{I})$.

Theorem 1. *The mapping Φ, defined by*

$$\Phi((c_i)_{i \in \mathbf{Z}})(x)$$

$$= \sum_{j=1}^{\infty} c_j A(n-1, 2j-1) \binom{x+j-1}{2j-1} + \sum_{j=0}^{\infty} c_{-j} A(n-1, 2j) \binom{x+j-1}{2j}$$

maps $\mathbf{Z}^{\mathbf{Z}}$ bijectively to $\mathsf{L}_n \mathsf{P}(\boldsymbol{I})$.

Note that the above sums are finite for any $x \in \mathbf{Z}$, because $j > |x|$ implies

$$\binom{x+j-1}{2j-1} = \binom{x+j-1}{2j} = 0 .$$

Before proving Theorem 2, we state two lemmas. The first one is taken from [5].

Lemma 1 ([5], Lemma 5). *For a function $f \colon \mathbf{Z} \to \mathbf{Z}$, the following, are equivalent.*

1. $f \in \mathsf{L}_n \mathsf{P}(\boldsymbol{I})$.

2. *For all y and for all $x_1, x_2, \ldots, x_{n-1} \in \mathbf{Z} \backslash \{y\}$ there exists a function $p \in \mathsf{P}(\boldsymbol{I})$ such that*

$$p(x_i) = \frac{f(x_i) - f(y)}{x_i - y} \quad \textit{for } i = 1, 2, \ldots, n-1 .$$

Now we construct some functions that lie in $\mathsf{L}_n P(\boldsymbol{I})$.

Lemma 2. *For $n \in \mathbf{N}$ and $i \in \mathbf{N}_0$ let $\beta_i^{(n)} \colon \mathbf{Z} \to \mathbf{Z}$ be defined by:*

$$\beta_i^{(n)} \colon x \mapsto \binom{x}{i} A(n-1, i) .$$

Then for all $n \in \mathbf{N}$ we have

$$\beta_i^{(n)} \in \mathsf{L}_n \mathsf{P}(\boldsymbol{I}) \qquad \forall i \in \mathbf{N}_0 . \tag{2.1}$$

Proof. We proceed by induction on n.

Base case $n = 1$. Since every function from $\mathbf{Z}$ into $\mathbf{Z}$ lies in $\mathsf{L}_1\mathsf{P}(\boldsymbol{I})$, so does every $\beta_i^{(1)}$.

Induction step $n \rightarrow n + 1$. For $i = 0$, we observe that $\beta_0^{(n)}$ is constant. But every constant function is clearly in $\mathsf{L}_n\mathsf{P}(\boldsymbol{I})$. Therefore, we will from now on assume that i is at least 1.

We have to show that $\beta_i^{(n)}$ lies in $\mathsf{L}_n\mathsf{P}(\boldsymbol{I})$. To this end, we show that $\beta_i^{(n)}$ satisfies condition 2 of Lemma 1. Let therefore y be any integer. Proceeding as in [7], we use the equality

$$\binom{x}{i} - \binom{y}{i} = \sum_{j=1}^{i} \binom{x-y}{j}\binom{y}{i-j}$$

for writing

$$\frac{\beta_i^{(n)}(x) - \beta_i^{(n)}(y)}{x-y} = \frac{\sum_{j=1}^{i} \binom{x-y}{j}\binom{y}{i-j} A(n-1, i)}{x-y}.$$

Hence for $x \neq y$ this is equal to

$$\sum_{j=1}^{i} \binom{y}{i-j}\binom{x-y-1}{j-1} \frac{A(n-1, i)}{j}.$$

In order to guarantee condition 2 of Lemma 1, it is sufficient to show that each summand lies in $\mathsf{L}_{n-1}\mathsf{P}(\boldsymbol{I})$. Since $A(n-1, j)$ divides $A(n-1, i)$ for $j \leqslant i$, this is guaranteed if the function f defined by

$$f(x) = \binom{x-y-1}{j-1} \frac{A(n-1, j)}{j}$$

lies in $\mathsf{L}_{n-1}\mathsf{P}(\boldsymbol{I})$ for $j = 1, 2, \ldots, i$.

In order to show this, we fix j with $1 \leqslant j \leqslant i$. By Definiton 1, $A(n-1, j)$ is a multiple of $jA(n-2, j-1)$. Since the induction hypothesis tells us that $g(x) = \binom{x-y-1}{j-1} A(n-2, j-1)$ lies in $\mathsf{L}_{n-1}\mathsf{P}(\boldsymbol{I})$, the function f lies in $\mathsf{L}_{n-1}\mathsf{P}(\boldsymbol{I})$ as well. This completes the induction step.

Now we are ready to prove the main result.

Proof of Theorem 1. Let $(z_i)_{i\in\mathbf{N}_0}$ be the enumeration of the integers given by $z_0=0$, $z_1=1$, $z_2=-1$, $z_3=2$ and, in general, $z_k=\frac{1}{2}(k+1)$ for odd k and $z_k=-\frac{1}{2}k$ for even k. By Z_i we denote the set $\{z_0, z_1, z_2, \ldots, z_{i-1}\}$. Let $g(n, i)$ be the generator of the ideal

$$\{l(z_i)\,|\,l\in \mathsf{L}_n P(\boldsymbol{I}) \text{ and } l(s)=0 \text{ for all } s\in Z_i\}$$

of the ring $\boldsymbol{I}$.

If we have a sequence $(b_i)_{i\in\mathbf{N}_0}\in \mathsf{L}_n \mathsf{P}(\boldsymbol{I})$ with the following *basis property*

$$b_i(s)=0 \text{ for all } s\in Z_i \text{ and } b(z_i)=g(n, i) \tag{2.2}$$

then we can easily convince ourselves that every $f\in \mathsf{L}_n \mathsf{P}(\boldsymbol{I})$ can be written as

$$f(x)=\sum_{i\in\mathbf{N}} a_i b_i(x)$$

where $a_i\in\mathbf{Z}$ for all $i\in\mathbf{N}_0$. Note that this sum is finite for any $x\in\mathbf{Z}$, because for $x=z_i$, we have $b_{i+1}(z_i)=b_{i+2}(z_i)=\ldots=0$. It is also obvious that each sequence $(a_i)_{i\in\mathbf{N}_0}$ gives rise to a function in $\mathsf{L}_n \mathsf{P}(\boldsymbol{I})$ and that different sequences produce different functions.

Hence we are done if we compute $g(n, i)$ and a sequence of functions b_i in $\mathsf{L}_n \mathsf{P}(\boldsymbol{I})$ with the *basis property* given in Condition (2.2).

First of all, we give a lower bound to $g(n, i)$ with respect to divisibility. In fact, we get

$$A(n-1, i)\,|\,g(n, i). \tag{2.3}$$

For proving Condition (2.3), we show that each product of at most $n-1$ elements in $\{1, 2, \ldots, i\}$ divides $g(n, i)$. We fix such a product $p=d_1\cdot d_2 \ldots d_{n_0-1}$, where $n_0\leqslant n$ and the d_k's are pairwise different members of $\{1, 2, \ldots, i\}$. Let l be a function in $\mathsf{L}_n P(\boldsymbol{I})$ with $l(s)=0$ for $s\in Z_i$. We show that the number p divides $l(z_i)$. Without loss of generality, we assume that i is odd, hence for $j=1, 2, \ldots, i$, the integer z_i-j is an element of Z_i.

Since $l\in \mathsf{L}_n \mathsf{P}(\boldsymbol{I})$, we find a polynomial function q on the integers such that q interpolates l at the places z_i-d_1, z_i-d_2, $z_i-d_3, \ldots, z_i-d_{n_0-1}$ and z_i. Since $q(z_i-d_j)=0$ for $j=1, 2, \ldots, n_0-1$, we know that we can write q in the form

$$q(x)=q_1(x)\prod_{j=1}^{n_0-1}(x-(z_i-d_j))$$

where q_1 is also a polynomial function with integral coefficients. Hence

$$l(z_i) = q(z_i) = q_1(z_i) \prod_{j=1}^{n_0 - 1} d_j .$$

Therefore $p = d_1 \cdot d_2 \dots d_{n_0 - 1}$ divides $l(z_i)$. This shows that $A(n-1, i)$ divides $g(n, i)$.

Lemma 2 now gives equality in Condition (2.3). Actually, Lemma 2 allows us to construct a sequence with the *basis property* given in Condition (2.2). For $j \in \mathbf{N}$ we define $s_j(x) = \binom{x+j-1}{2j-1} A(n-1, 2j-1)$ and for $j \in \mathbf{N}_0$ we let $t_j(x) = \binom{x+j-1}{2j} A(n-1, 2j)$. The sequence $(t_0, s_1, t_1, s_2, t_2, s_3, \dots)$ has the properties required in (2.2). In addition, by Lemma 2, all s_j and t_j are in $\mathsf{L}_n \mathsf{P}(\boldsymbol{I})$.

We shall now prove that the example of an element in $\mathsf{L}_n \mathsf{P}(\boldsymbol{I}) \backslash \mathsf{L}_{n+1} \mathsf{P}(\boldsymbol{I})$ given in [5] is actually the easiest possible one.

Corollary 1. *Let p be a polynomial function on the rational numbers with rational coefficients such that the restriction of p to the integers lies in $\mathsf{L}_n \mathsf{P}(\boldsymbol{I})$, but not in $\mathsf{L}_{n+1} \mathsf{P}(\boldsymbol{I})$. Then the degree of p is at least $2n$.*

Proof. We have $A(n, j) = j!$ for $j \leq 2n+1$ and $A(n, 2n+2) = \dfrac{(2n+2)!}{2}$. Hence for $j < 2n$ we have $A(n, j) = A(n-1, j) = j!$, but $A(n, 2n) \neq A(n-1, 2n)$.

3 - A remark on the cardinality of $\mathsf{L}_n F$

In [6], W. Nöbauer proposes to investigate the cardinalities of the sets $\mathsf{L}_n P(\boldsymbol{A})$ for all kinds of universal algebras $\boldsymbol{A}$. In this section, we give an elementary reason for the fact that $\mathsf{LP}(\boldsymbol{I})$ is uncountable.

Convention 1. For the rest of this note, let $\boldsymbol{G} = \langle G; +, -, 0 \rangle$ be a group, and let $\boldsymbol{F}$ be a subgroup of $\boldsymbol{G}^G$. The carrier set of $\boldsymbol{F}$ is, as usual, denoted by F.

Definition 2. Let $\boldsymbol{F}$, $\boldsymbol{G}$ be as in Convention 1. Then D is a *base of equality* for F iff $D \subseteq G$ and every function in F that is zero at all elements of D is zero everywhere on G.

The following proposition is an obvious modification of [2], Lemma 1.

Proposition 2. *Let G and F be as in Convention 1, and let D be a base of equality for F. Let n be the cardinality of D. Then we have* $\mathsf{L}_{n+1}F = F$.

Proof. We suppose that there is a function l that lies in $\mathsf{L}_{n+1}F$, but not in F. Since l is in $L_{n+1}F$, there is a function $f_1 \in F$ that agrees with l on D. Since f_1 lies in F, but l does not, we have a point $y \in G$ such that $f_1(y) \neq l(y)$. The cardinality of $D \cup \{y\}$ is $n+1$, hence there is a function $f_2 \in F$ that agrees with l on $D \cup \{y\}$. Therefore the functions f_1 and f_2 agree on D, but they have different values at y. Hence the function $f_1 - f_2$ is zero everywhere on D, but not the zero function. This contradicts the fact that D is a base of equality of F.

Note that Proposition 2 is also true for infinite cardinals n. Of course, in this case we have $n+1=n$.

We will now give a result that can be considered as a reversion of this proposition.

Theorem 2. *Let G and F be as in Convention 1. If F and G are both countable and if $F = \mathsf{L}F$ then there exists a finite base of equality D for F.*

Proof. The result is obvious if F or G is finite. Let $\gamma_0, \gamma_1, \gamma_2, \dots$ and $f_0, f_1, f_2, \dots$ be complete enumerations of F and G, respectively. Furthermore we abbreviate the set $\{\gamma_i \mid i \leq r\}$ by $\Gamma(r)$.

Suppose that there is no finite base of equality for F. We shall construct a sequence $(n_m)_{m \in \mathbf{N}_0}$ of non-negative integers and a sequence $(g_m)_{m \in \mathbf{N}_0}$ of elements of F with the properties:

1. $g_m|_{\Gamma(n_m)} \neq f_m|_{\Gamma(n_m)} \quad \forall m \in \mathbf{N}_0$
2. $n_{m+1} > n_m \quad \forall m \in \mathbf{N}_0$
3. $g_{m+1}|_{\Gamma(n_m)} = g_m|_{\Gamma(n_m)} \quad \forall m \in \mathbf{N}_0$.

We construct the sequences inductively. Let $g_0 \in F$ such that $g_0 \neq f_0$. Let n_0 be minimal in $\mathbf{N}_0$ with $g_0(\gamma_{n_0}) \neq f_0(\gamma_{n_0})$.

If we have already constructed g_m and n_m we construct g_{m+1} and n_{m+1} as follows:

In the case $g_m|_{\Gamma(n_m)} = f_{m+1}|_{\Gamma(n_m)}$ there exists a function $h \in F$ with $g_m|_{\Gamma(n_m)} = h|_{\Gamma(n_m)}$ and $h \neq f_{m+1}$, since otherwise $\Gamma(n_m)$ would be a forbidden base of equality for F. We set $g_{m+1} = h$. Now let n_{m+1} be minimal with $h(\gamma_{n_{m+1}}) \neq f_{m+1}(\gamma_{n_{m+1}})$.

If $g_m|_{\Gamma(n_m)} \neq f_{m+1}|_{\Gamma(n_m)}$, we set $g_{m+1} = g_m$ and $n_{m+1} = n_m + 1$.

Since for every $\gamma \in G$, the sequence $(g_m(\gamma))_{m\in \mathbf{N}}$ is eventually constant, we may define a function l on G by

$$l(\gamma) = \lim_{m\to\infty} g_m(\gamma).$$

The function l lies in $\mathsf{L}F$, and hence, by assumption, l lies in F. So l is equal to f_m for some $m \in \mathbf{N}_0$. Since $l|_{\Gamma(n_m)} = g_m|_{\Gamma(n_m)}$ and $g_m|_{\Gamma(n_m)} \neq f_m|_{\Gamma(n_m)}$, we obtain $l|_{\Gamma(n_m)} \neq f_m|_{\Gamma(n_m)}$. But this shows that l can not be equal to f_m.

Putting the last two propositions together, we get

Corollary 2. *Let* $\boldsymbol{G}$ *and* $\boldsymbol{F}$ *be as in Convention* 1. *If* F *and* G *are both countable and if* $F = \mathsf{L}F$ *then there exists an* $n \in \mathbf{N}_0$ *such that* $F = \mathsf{L}_n F$.

This property can be strengthened.

Corollary 3. *Let* $\boldsymbol{G}$ *and* $\boldsymbol{F}$ *be as in Convention* 1. *If* $\mathsf{L}F$ *and* G *are both countable, then we have:*

1. *There is a finite base of equality* D *for* F.
2. $\mathsf{L}F = F$.

Proof. By the idempotence of the operator L, we have $\mathsf{L}F = \mathsf{L}\mathsf{L}F$. Since both $\mathsf{L}F$ and G are countable, we may apply Theorem 2 and get a finite base of equality D for $\mathsf{L}F$. Since F is a subset of $\mathsf{L}F$, the set D is also a base of equality of F. This proves (1); the claim in (2) now follows by Proposition 2.

Corollary 4. *Let* $\boldsymbol{R}$ *be a countably infinite integral domain. Then* $\mathsf{LP}(\boldsymbol{R})$ *is not countable.*

Proof. We suppose that $\mathsf{LP}(\boldsymbol{R})$ is countable. Then there exists a finite base of equality D for $\mathsf{P}(\boldsymbol{R})$, and hence the polynomial $p(x) = \prod_{d\in D}(x-d)$ induces the zero-function on R. This is impossible because $\boldsymbol{R}$ is an infinite integral domain.

For polynomial functions on Ω-groups, we obtain the following corollary. We recall that Ω-groups are groups with further operations; a definition is given, e.g., in [3].

Corollary 5. *Let* $\boldsymbol{V}$ *be an* Ω*-group. If* $\mathsf{LP}(V)$ *is countable, then there exists a finite base of equality for* $\mathsf{P}(\boldsymbol{V})$.

Proof. The result follows from Corollary 3 and the observation that LP(V) can only be countable if V is countable as well.

References

[1] R. R. HALL, *On pseudo-polynomials*, Mathematika 18 (1971), 71-77.

[2] H. HULE and W. NÖBAUER, *Local polynomial functions on universal algebras*, An. Acad. Brasil. Cienc. 49 (1977), 365-372.

[3] A. G. KUROSH, *Lectures on general algebra*, Chelsea, New York 1965.

[4] H. LAUSCH and W. NÖBAUER, *Algebra of polynomials*, North-Holland, Amsterdam 1973.

[5] H. LAUSCH and W. NÖBAUER, *Local polynomial functions on factor rings of the integers*, J. Austral. Math. Soc. 27 (1979), 232-238.

[6] W. NÖBAUER, *Local polynomial functions: results and problems*, Tech. Univ. Wien 1978, preprint.

[7] I. RUSZA, *On congruence preserving functions*, Mat. Lapok 22 (1971), 125-134.

Sommario

Si determinano tutte le funzioni sull'insieme **Z** *degli interi relativi che possono essere interpolate da un polinomio a coefficienti in* **Z** *su ogni sottoinsieme di* **Z** *con al più n punti. Inoltre si dimostra che in ogni dominio di integrità esistono molte funzioni che si comportano localmente come polinomi sebbene polinomi non siano.*

* * *